EXHIBIT 1

Memo., John Ratcliffe, Director of National *Intelligence, Views on Intelligence Community Election Security Analysis* (Jan. 7, 2021)

UNCLASSIFIED

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC

SUBJECT: Views on Intelligence Community Election Security Analysis

REFERENCE: Intelligence Community Assessment, Foreign Threats to the 2020 U.S. Elections

From my unique vantage point as the individual who consumes all of the U.S. government's most sensitive intelligence on the People's Republic of China, I do not believe the majority view expressed by Intelligence Community (IC) analysts fully and accurately reflects the scope of the Chinese government's efforts to influence the 2020 U.S. federal elections.

The IC's Analytic Ombudsman issued a report, which I will reference several times below, that includes concerning revelations about the politicization of China election influence reporting and of undue pressure being brought to bear on analysts who offered an alternative view based on the intelligence. The Ombudsman's report, which is being transmitted to Congress concurrently with this Intelligence Community Assessment (ICA), also delves into a wider range of election security intelligence issues that I will not focus on here. However, the specific issues outlined below with regard to China reporting are illustrative of broader concerns. It is important for all IC leaders to foster a culture within the Community that encourages dissenting views that are supported by the intelligence. Therefore, I believe it is incumbent upon me in my role as the Director of National Intelligence to lead by example and offer my analytic assessment alongside the majority and minority views. This letter was prepared in consultation with the Ombudsman to ensure that I am accurately articulating his findings and presenting them in their proper context.

The majority view expressed in this ICA with regard to China's actions to influence the election fell short of the mark for several specific reasons.

Analytic Standard II requires the IC to maintain "independence of political considerations." This is particularly important during times when the country is, as the Ombudsman wrote, "in a hyper partisan state." However, the Ombudsman found that

> "China analysts were hesitant to assess Chinese actions as undue influence or interference. These analysts appeared reluctant to have their analysis on China brought forward because they tend to disagree with the administration's policies, saying in effect, I don't want our intelligence used to support these policies. This behavior would constitute a violation of Analytic Standard II: Independence of Political Considerations (IRTPA Section 1019)."

Furthermore, alternative viewpoints on China's election influence efforts have not been appropriately tolerated, much less encouraged. In fact, the Ombudsman found that

UNCLASSIFIED

[redacted]

SUBJECT: [redacted]

[redacted]

[redacted]

[

[redacted]

[redacted] Terms of Intelligence Community Director Reality Analysis

[redacted] I have ordered the IC to provide me a Right Our Reality Analysis which has been designed.

[redacted]

[redacted]

[redacted]

[redacted]

EXHIBIT 2

Letter from Pamela S. Karlan, Principal Deputy Assistant Attorney General, Civil Rights Division, to Arizona Sen. Karen Fann (May 5, 2021)

U.S. Department of Justice
Civil Rights Division

May 5, 2021

VIA EMAIL

The Honorable Karen Fann
President, Arizona State Senate
1700 West Washington Street, Room 205
Phoenix, AZ 85007

Dear Senator Fann:

I write regarding issues arising under federal statutes enforced by the United States Department of Justice that are related to the audit required by the Arizona State Senate for the November 2020 federal general election in Maricopa County. News reports indicate that the Senate subpoenaed ballots, elections systems, and election materials from Maricopa County and required that they be turned over to private contractors, led by a firm known as Cyber Ninjas.

The Department has reviewed available information, including news reports and complaints regarding the procedures being used for this audit. The information of which we are aware raises concerns regarding at least two issues of potential non-compliance with federal laws enforced by the Department.

The first issue relates to a number of reports suggesting that the ballots, elections systems, and election materials that are the subject of the Maricopa County audit are no longer under the ultimate control of state and local elections officials, are not being adequately safeguarded by contractors at an insecure facility, and are at risk of being lost, stolen, altered, compromised or destroyed.[1] Federal law creates a duty to safeguard and preserve federal election records. The Department is charged with enforcement of provisions of the Civil Rights Act of 1960, 52 U.S.C. §§ 20701-20706. This statute requires state and local election officials to maintain, for twenty-two months after the conduct of an election for federal office, "all records and papers" relating to any "act requisite to voting in such election…" *Id.* at § 20701. The purpose of

[1] *See, e.g.*, https://www.azfamily.com/news/investigations/cbs_5_investigates/security-lapses-plague-arizona-senates-election-audit-at-state-fairgrounds/article_b499aee8-a3ed-11eb-8f94-bfc2918c6cc9.html; https://www.azmirror.com/2021/04/23/experts-raise-concerns-about-processes-transparency-as-election-audit-begins/; https://tucson.com/news/local/arizona-senate-issues-subpoena-demanding-access-to-2-million-plus-ballots-cast/article_a426fc7b-60d8-5837-b244-17e5c2b2ddb4.html; https://www.azmirror.com/2021/02/26/judge-sides-with-senate-says-maricopa-must-turn-over-election-materials-for-audit/

these federal preservation and retention requirements for elections records is to "secure a more effective protection of the right to vote." *State of Ala. ex rel. Gallion v. Rogers*, 187 F. Supp. 848, 853 (M.D. Ala. 1960*), aff'd sub nom. Dinkens v. Attorney General*, 285 F.2d 430 (5th Cir. 1961) (per curiam), *citing* H.R. Rep. 956, 86th Cong., 1st Sess. 7 (1959); *see also* Federal Prosecution of Election Offenses, Eighth Edition 2017 at 75 (noting that "[t]he detection, investigation, and proof of election crimes – and in many instances Voting Rights Act violations – often depend[s] on documentation generated during the voter registration, voting, tabulation, and election certification processes").[2]

If the state designates some other custodian for such election records, then the Civil Rights Act provides that the "duty to retain and preserve any record or paper so deposited shall devolve upon such custodian." 52 U.S.C. § 20701. The Department interprets the Act to require that "covered election documentation be retained either physically by election officials themselves, or under their direct administrative supervision." *See* Federal Prosecution of Election Offenses at 79. In addition, if the state places such records in the custody of other officials, then the Department views the Act as requiring that "administrative procedures be in place giving election officers ultimate management authority over the retention and security of those election records, including the right to physically access" such records. *Id*. We have a concern that Maricopa County election records, which are required by federal law to be retained and preserved, are no longer under the ultimate control of elections officials, are not being adequately safeguarded by contractors, and are at risk of damage or loss.

The second issue relates to the Cyber Ninjas' statement of work for this audit.[3] Among other things, the statement of work indicates that the contractor has been working "with a number of individuals" to "identify voter registrations that did not make sense, and then knock on doors to confirm if valid voters actually lived at the stated address." Statement of Work at ¶ 2.1. The statement of work also indicates that the contractor will "select a minimum of three precincts" in Maricopa County "with a high number of anomalies" in order "to conduct an audit of voting history" and that voters may be contacted through a "combination of phone calls and physical canvassing" to "collect information of whether the individual voted in the election" in November 2020. Statement of Work at ¶ 5.1. This description of the proposed work of the audit raises concerns regarding potential intimidation of voters. The Department enforces a number of federal statutes that prohibit intimidation of persons for voting or attempting to vote. For example, Section 11(b) of the Voting Rights Act provides that "No person, whether acting under color of law or otherwise, shall intimidate, threaten, or coerce, or attempt to intimidate, threaten, or coerce any person for voting or attempting to vote, or intimidate, threaten, or coerce, or attempt to intimidate, threaten, or coerce any person for urging or aiding any person to vote or attempt to vote…" 52

[2] *See* https://www.justice.gov/criminal/file/1029066/download

[3] *See* https://www.washingtonpost.com/context/cyber-ninjas-statement-of-work/2013a82d-a2cf-48be-8e9f-a26bfd5143e5/

U.S.C. § 10307(b). Past experience with similar investigative efforts around the country has raised concerns that they can be directed at minority voters, which potentially can implicate the anti-intimidation prohibitions of the Voting Rights Act. Such investigative efforts can have a significant intimidating effect on qualified voters that can deter them from seeking to vote in the future.

We would appreciate your response to the concerns described herein, including advising us of the steps that the Arizona Senate will take to ensure that violations of federal law do not occur.

Sincerely,

Pamela S. Karlan
Principal Deputy Assistant Attorney General
Civil Rights Division
pamela.karlan@usdoj.gov

cc: Glenn McCormick, Acting United States Attorney for the District of Arizona
Mark Brnovich, Arizona Attorney General
Katie Hobbs, Arizona Secretary of State
Stephen Richer, Maricopa County Recorder

EXHIBIT 3

Caltech/MIT Voting Technology Project, Summary Report, Election Auditing, Key Issues and Perspectives (2018)

ELECTION AUDITING

KEY ISSUES AND PERSPECTIVES

SUMMARY REPORT

MIT ELECTION DATA + SCIENCE LAB

Caltech/MIT Voting Technology Project

ELECTION AUDIT SUMMIT
DECEMBER 7-8, 2018

ACKNOWLEDGMENTS

The coordinators of this summary report extend their deepest appreciation to each of the panelists who participated in the Election Audit Summit, without whom this report could not have taken form, and to all those involved in making the event and this report possible, especially Claire DeSoi, Daniel Guth, and Kathryn Treder. They also gratefully acknowledge the many attendees of that summit, who continue to advance the conversation on election administration and auditing in the United States.

DISCLAIMER

The findings, interpretations, and conclustions expressed in this report do not necessarily represent the views or opinions of the California Institute of Technology or the Massachusetts Institute of Technology.

The Caltech/MIT Voting Technology Project and the MIT Election Data & Science Lab encourage dissemination of knowledge and research; this report may be reproduced in whole or in part for non-commercial or educational purposes so long as full attribution to its authors is given.

PREFACE

On December 7 and 8, 2018, The Caltech/MIT Voting Technology Project (VTP) hosted the Multidisciplinary Conference on Election Auditing, or "Election Audit Summit," for short, at the Massachusetts Institute of Technology in Cambridge, Massachusetts. The conference was organized by a small group of academics and practitioners from across the United States:

- R. Michael Alvarez (Caltech)
- Jennifer Morrell (Democracy Fund, Election Validation Project)
- Ronald Rivest (MIT)
- Philip Stark (UC Berkeley)
- Charles Stewart III (MIT)

Inspired by the groundswell of interest in risk-limiting audits and other rigorous methods to ensure that elections are properly administered, the conference assembled an eclectic mix of academics, election officials, and members of the public to explore these issues. The essays in this report briefly summarize many of the presentations made at the Audit Summit, while the first chapter ties together the themes of the Summit into one package.

A permanent record of the conference, including video of all the sessions, exists online at https://electionlab.mit.edu/election-audit-summit.

TURN OVER FOR PAGE

CONTENTS

PREFACE c

INTRODUCTION: THOUGHTS FROM THE ELECTION AUDIT SUMMIT iii
CHARLES STEWART III
R. MICHAEL ALVAREZ

CURRENT STATUS OF POST-ELECTION AUDITING AND RECOUNT PRACTICES

RISK-LIMITING AUDITS AND EVIDENCE-BASED ELECTIONS 2
PHILIP B. STARK

COMPREHENSIVE ELECTION PERFORMANCE AUDITING 5
R. MICHAEL ALVAREZ

ELECTION VALIDATION PROJECT 8
JENNIFER MORRELL

POST-ELECTION AUDITS: THE STATE OF THE STATES 12
DYLAN LYNCH

NEW STATISTICAL APPROACHES TO AUDITING VOTE TABULATION AND RECOUNTS

SAMPLING WITH *K*-CUT, AND BAYESIAN AUDITS 17
RONALD L. RIVEST

ELECTION FORENSICS BEYOND AUDITS 21
WALTER R. MEBANE, JR

NEW STATISTICAL TECHNIQUES IN INTERNATIONAL PERSPECTIVE 25
EMILY BEAULIEU BACCHUS

WHAT COLORADO CAN TEACH US ABOUT POST-ELECTION AUDITS

RISK-LIMITING AUDITS: LESSONS LEARNED 30
NEAL MCBURNETT

SUMMARY OF RLA IMPLEMENTATION: TRAINING & CHANGE MANAGEMENT 34
HILARY RUDY

LOOKING BEYOND COLORADO: CHANGING TECHNOLOGY AND STATE POLICY

LOOKING BEYOND COLORADO: RISK LIMITING AUDITS IN INDIANA 38
JAY BAGGA
BRYAN BYERS

VOTING TECHNOLOGY & POST-ELECTION AUDITS 42
JEROME LOVATO

SOFTWARE SUPPORT FOR RISK-LIMITING AUDITS 45
MARK LINDEMAN

NEW DIRECTIONS FOR COMPREHENSIVE AUDITING AND FORENSICS

AUDITING THE ASSIGNMENT OF REGISTERED VOTERS TO DISTRICTS 49
BRIAN AMOS
MICHAEL MCDONALD

PUBLICLY-VERIFIABLE ELECTIONS 52
JOSH BENALOH

DESIGNING BALLOTS FOR VOTERS AND ELECTION WORKERS—AND AUDITS 55
WHITNEY QUESENBERY

FURTHER READING 59

INTRODUCTION: THOUGHTS FROM THE ELECTION AUDIT SUMMIT

CHARLES STEWART III
Massachusetts Institute of Technology

R. MICHAEL ALVAREZ
California Institute of Technology

For nearly twenty years Americans have been faced with questions about the integrity of their country's elections. Challenges to election integrity arise for a variety of reasons, ranging from bad luck, to mistakes, to malicious behavior. The possibility that something might happen in the conduct of an election that might place the correctness of its conclusions at risk have led many to ask the question:

> *"How do we know that the election outcomes announced by election officials are correct?"*

Ultimately, the only way to answer a question like this is to rely on procedures that independently review the outcomes of elections, to detect and correct material mistakes that are discovered. In other words, elections need to be audited.

But how?

The broad topic of auditing elections was the subject of the Election Audit Summit, a public conference held at the Massachusetts Institute of Technology in December 2018. This report presents a summary of the viewpoints presented at that conference. This introductory chapter frames the issues that brought the conference together and presents some summary thoughts about how the practice of auditing can be more thoroughly incorporated into the practice of administering elections in the United States.

From the outset, it should be said that the purpose of the Summit was not solely to share ideas about auditing. A second purpose was to help build bridges between academic researchers and practitioners in the elections field—communities that have of-

ten been at loggerheads over the need for, and proper scope of, election auditing.

We believe the conference was a success, both on the intellectual and community-building fronts. Evidence of that success—at least on the intellectual side—is contained within the covers of this report.

The short papers that follow contain summaries of nearly all the presentations made at the conference. These papers range across a variety of topics, including theoretical and practical issues related to post-election tabulation audits, audits of non-tabulation processes, changes needed in the legal and business environments to accommodate the greater implementation of election audits, and applications of audits to settings outside the United States.

Readers of this report who want more than what is contained in this report are invited to visit the conference website, where slides from the presentations and videos of all panels are located. The URL for that website is https://electionlab.mit.edu/election-audit-summit.

The rest of this chapter provides an introduction to the issues addressed at the conference and in the rest of this report. It is organized around eight questions:

- What are audits for?
- Why do we need audits?
- What do we want to audit?
- Who should do audits?
- Why should people believe the results of post-election audits?
- How often are audits needed?
- How do we get states and counties to implement election audits?
- What can Americans learn about auditing from other countries?

WHAT ARE AUDITS FOR?

Election audits are intended to accomplish two things. The first is to ensure that the election was properly conducted, that election technologies performed as expected, and that the correct winners were declared. The second is to convince the public of the first thing. ***Convincing the public*** that the election was properly conducted and that the correct winners were declared is a core activity of establishing legitimacy in a democracy.

Of course, whether audits actually instill confidence is an empirical question. There is scant research into whether post-election audits in the United States actually serve this legitimating purpose. And, indeed, as Emily Beaulieu's presentation and essay in this report demonstrate, there are cases in overseas elections where the process of election scrutiny has undermined public confidence in those elections.

Still, the purpose of the Summit was to help the nation move ahead in applying higher quality control standards to the conduct of elections. As the presentations and the discussion made abundantly clear, it is insufficient simply to develop fine-tuned and scientifically justified modes of auditing. It is also necessary to develop communications plans, so that the public understands the purpose and processes behind these audits, that the results of any auditing are available to stakeholders and the public, and that the conduct of audits becomes part of the pride a community has in conducting clean elections.

WHY DO WE NEED AUDITS?

Solid evidence can be adduced that elections in the United States have become, on the whole, better-run since the 2000 presidential election highlighted serious shortcomings in vote tabulation, ballot design, voter registration, mail-ballot administration, poling-place operations, and recount laws. At the same time, the shortcomings identified in 2000 have only been incompletely addressed, as new challenges—such as cybersecurity threats and aging voting equipment—have emerged.

One result is that although Americans remain as confident that their own ballots are counted as intended as they were in the early 2000s, their confidence in the vote-count nationwide has fallen steadily since then.[1] Following the 2018 election, approximately 40% of respondents to a post-election academic poll stated that people breaking into election computer systems and voting equipment was either a "major problem" or "a problem."[2] Furthermore, although most Americans are confident that the voting equipment they use is hard to hack, recent criticism of electronic voting equipment has led to a decline in support for those systems.[3]

Moving beyond confidence in the vote and the voting equipment, recent stories emanating from the 2017 and 2018 elections show what happens when attention to all the details that make up an election are not carefully attended to. For instance, in a 2017 state legislative election that determined which party would control the Virginia House of Delegates, it was discovered that 26 voters in that district had been incorrectly assigned to vote in that district.[4] The 2018 U.S. Senate race in Florida may have been determined by poor ballot layout in parts of Broward County.[5] In 2018 there were a number of reported SNAFUS with respect to California's new "motor voter" registration process, in particular regarding how the state's Department of Motor Vehicles was collecting and processing voter registration and re-registration requests, and reports that the registration system itself may have been the target of hackers.[6]

Events like these illustrate why it is important for states and localities to engage in comprehensive programs of auditing and quality assurance for every aspect of election management. Election margins are as close these days as they have been in American history; with partisan polarization, small electoral margins can produce huge policy swings. A lot is riding on getting all the details right, and on communicating that to stakeholders and voters.

---

[1] Michael W. Sances and Charles Stewart III. "Partisanship and confidence in the vote count: Evidence from US national elections since 2000." Electoral Studies 40 (2015): 176–188; Betsy Sinclair, Steven S. Smith, and Patrick D. Tucker. "'It's Largely a Rigged System:' Voter Confidence and the Winner Effect in 2016," Political Research Quarterly 71, no. 4 (2018): 854–868.

[2] These findings are based on responses to the MIT module of the 2018 Cooperative Congressional Election Study (CCES).

[3] Charles Stewart III and Dunham, James, "Attitudes toward Voting Technology, 2012–2018." Paper presented at the annual meeting of the Midwest Political Science Association, April 4–7, 2019. Available at SSRN: https://ssrn.com/abstract=3363708 or http://dx.doi.org/10.2139/ssrn.3363708.

[4] Laura Vozzella and Ted Mellnik, "Va. election officials assigned 26 voters to the wrong district. It might've cost Democrats a pivotal race." *Washington Post,* May 13, 2018.

[5] Larry Barszewski , Lois K. Solomon , Rafael Olmeda and Skyler Swisher, "Broward recount appears to confirm thousands skipped voting in hotly contested Senate race," *South Florida Sun Sentinel,* Nov. 16, 2018.

[6] John Myers, "Hackers attacked California DMV voter registration system marred by bugs, glitches." *Los Angeles Times*, April 9, 2019.

WHAT DO WE WANT TO AUDIT? (EXPANDING THE CONCEPT OF AN AUDIT)

Formal audits of vote tabulations have been occurring in the United States ever since California mandated post-election audits in the 1960s. By the 2018 election, roughly 30 states required some form of post-election tabulation audit. The typical form of these audits is to require a hand recount of the ballots in a fixed percentage of precincts, usually 1%. These percentages vary considerably across states and, of course, there is still a substantial minority of states with no requirement for post-election tabulation audits at all.

A lot has changed in elections since the 1960s, and this is reflected in advances in the practice and theory of election auditing. Dylan Lynch's contribution to this report discusses the state of auditing requirements across the states, as of late 2018.[7]

Among the audit topics covered in the conference and in this report are the following:

Risk-limiting audits (RLA). An RLA is a post-election tabulation audit in which a random sample of voted ballots is manually examined for evidence that the originally reported outcome of the election is correct.[8] The RLA examines an increasing number of ballots until there is sufficiently strong evidence that looking at all ballots would show that the originally reported outcome is correct. In the limiting case, which is likely to be rarely encountered, all ballots must be examined, as in a recount. If the originally reported outcome is in fact incorrect, there is a pre-specified minimum chance that the audit will correct the result. The correction is made by performing a full manual tally. As its name suggests, an RLA limits the risk of certifying a contest with the wrong winner.

Much of this report concerns RLAs. Philip Stark's essay on "RLAs and Evidence-Based Elections" provides a grounding in the general topic of RLAs.[9] Essays by Neal McBurnett and Hillary Rudy, that arise out of the experience with RLAs in Colorado, provide insightful comments from experienced practitioners.[10] The essay by Jay Bagga and Bryan Byers provides insights into RLA pilots conducted in Indiana — a state that currently has no statewide post-election audit requirement of any sort.[11]

Auditing who gets which ballot. Ballots in the United States are the longest in the world, at least when measured by the number of offices and questions (referenda and initiatives) that appear on the ballots. This is only partly because of federalism and the need to elect officials at three levels of government, federal, state, and local. It is also because state and local governments put offices on the ballot that in other countries would be appointed by the governing authorities. Members of the U.S. House of Representatives and many state and local officials are elected in districts. These

[7] Lynch's presentation at the Summit may be found at 48:08 of the conference video: https://youtu.be/t-cYEVOKWxc?t=2888.

[8] Here, *correct* means that an accurate manual tabulation of all validly cast ballots would give the same winner(s). RLAs can correct tabulation errors, but assume the paper trail is trustworthy; establishing this would take the form of a ***compliance audit***.

[9] Stark's presentation may be found at 26:20 of the conference video: https://youtu.be/t-cYEVOKWxc?t=1580. Ronald Rivest's presentation addressed new developments in the area of RLAs: https://youtu.be/kY5siXsgWUI?t=116.

[10] The panel on the Colorado experience may be found on the conference video here: https://youtu.be/1cbElHGePrA.

[11] The panel on "Looking beyond Colorado" may be found on the conference video here: https://youtu.be/r4jX6CVeBpk.

districts overlap one another in haphazard ways. It is usually the case that the unique combination of offices and questions that appear on the ballot in one precinct are different from the neighboring precinct. To ensure that voters vote on the correct matters—that is, are given the correct ballot—requires careful attention to detail among state and local officials.

The Summit presentation of Michael McDonald, from the University of Florida, powerfully made the case that that voters are oftentimes given the wrong ballot, because the legal definitions of precincts do not always align with geography.[12] These problems can be caused by a number of reasons. For instance, states that define districts using Census Bureau geography often don't account for the fact that the definitions of this geography can change between decennial censuses. Or, addresses may be improperly geo-coded. McDonald makes a strong argument for periodic auditing of the assignment of voters to districts, and that states and localities do a better job at collecting data on district boundaries.

Auditing ballot design. Many of the people who are now academic leaders in the study of voting technology got their start because of the poor ballot design in Florida during the 2000 presidential election. As Whitney Quesenbery, of the Center for Civic Design, points out in her contribution to this report, history has shown that poorly designed ballots, including hand-marked and –verified ballots, can mislead voters.[13] Organizations like the Center for Civic Design have made election officials aware of ballot-design best practices,[14] and these best practices have been disseminated by the EAC.[15] But, even well-intended ballots may hold unanticipated problems, which raises the importance of pre-testing ballots on humans. It also suggests an opening for vendors and civic tech groups to create applications to help test ballot designs against these practices.

Auditing everything else. The essay by R. Michael Alvarez in this report contains the most direct expression of the need to "audit everything."[16] Noting the importance of procedures such as logic-and-accuracy tests and post-election audits, Alvarez writes that, nonetheless:

> *a "logic and accuracy" test of voting equipment used for in-person ballot marking on Election Day or in a vote center doesn't shed any light on the integrity of a jurisdiction's voting-by-mail process, nor does a post-election ballot audit help us determine the integrity or accuracy of a jurisdiction's voter registration process and databases. For a more complete assessment of the integrity of an election in a state or county, we need different and more comprehensive methodologies that can evaluate the performance of the entire election jurisdiction's "eco-system."*

[12] McDonald's presentation may be found at 43:23 of the conference video: https://youtu.be/eFks-xHZH5o?t=2603.

[13] Quesenbery's presentation may be found at 1:06:21 of the conference video: https://youtu.be/eFks-xHZH5o?t=3981.

[14] https://civicdesign.org/fieldguides/

[15] https://www.eac.gov/election-officials/designing-polling-place-materials/.

[16] Alvarez's presentation may be found at 25:59 of the conference video: https://youtu.be/eFks-xHZH5o?t=1559.

In the spirit of this quote, Alvarez discusses a comprehensive assessment project he and his students at Caltech undertook during the 2018 primaries and general election in Orange County, California to assess a variety of election procedures, ranging from mail-ballot transmission to voter registration accuracy, to the monitoring of social media.

WHO SHOULD DO AUDITS?

As audits become regarded as more of a central feature to election administration, an important question emerges: who does the auditing? Presently, post-election audits are typically conducted by the authorities who conduct the elections, with the State of Connecticut being a notable exception.[17] However, it is conceivable (some might even say advisable) that post-election auditing be done by independent third parties.

Taking the lead from the world of finance, there would seem to be advantages to establishing independent election audit boards. Related to this point, Bill Kresse, a CPA who teaches auditing and financial forensics, made the point at the last Summit panel that all states have financial auditors who could supply an instant and willing army of individuals who would be at home in the world of ballot-level audits.[18]

Unfortunately, most jurisdictions seem unwilling to go the next step to establish completely independent auditing procedures, but that does not mean these jurisdictions are unresponsive to the need to "guard the guardians." For instance, as was noted in the Summit panel that reviewed Colorado's experience implementing post-elect auditing, even though election workers were the ones who provided the person-power to audit the results, they did not know which ballots would be reviewed until the audit began. (Furthermore, all stages of the post-election audit were viewed by the public.)

Taking a step away from the formal auditing process, the Summit raised the issue of the public reviewing the results of the election and effectively crowdsourcing an audit. The case of North Carolina's 9th congressional district in 2018 is close to an example of this. In that election, Republican Mark Harris initially appeared to beat Democrat Dan McCready by 905 votes. However, stories quickly emerged alleging absentee-ballot irregularities in Bladen County that were orchestrated by Republican political operative McRae Dowless. After a hearing by the North Carolina State Board of Elections (NCSBOE), the board failed to certify the election because of the irregularities and called a new election.

A lot went into the charges of irregularities and the investigation that ensued. Certainly, one factor that helped the charges gain traction is the fact that the NCSBOE maintains one of the most complete election data sites in the country that include detailed data files that document the request, distribution, return, and resolution of every mail ballot requested in the state. This allowed state investigators, journalists, academics, and citizen enthusiasts to search the record on their own, not only to confirm what officials were finding, but to examine whether there were instances of "District Nine behavior." The 9th CD episode illustrates the importance of making administrative

[17] The Center for Voting Technology Research (VoTeR) at the University of Connecticut. Audit reports are contained at this Web site: https://voter.engr.uconn.edu/voter/audits/.

[18] Kresse's presentation may be found at 41:44 of the conference video: https://youtu.be/LLNX-0eJ9JmU?t=2504.

data from elections available to the public in a usable format, and also illustrates that wrongdoing can sometimes be detected outside of formal post-election auditing programs.

WHY SHOULD PEOPLE BELIEVE THE RESULTS OF POST-ELECTION AUDITS?

A criticism made of states that have no requirements for post-election auditing is that they provide no way for the public to be assured that election outcomes are the correct ones, other than accept election officials when they say, "trust us." The promise of more sophisticated techniques, such as risk-limiting audits, is that they not only require a strict adherence to chain-of-custody and auditing protocols, but they can provide a mathematically rigorous away to quantify how confident we should be that election results are correct.

There are problems with both sets of claims made in the preceding paragraph, of course. As to the criticism that the lack of a formal program of post-election auditing leaves candidates and the public simply to trust election administrators, it can be said that even states that do not require audits have practices that allow for independent observation of polling places, vote counting, tabulation, and canvassing. All states allow close elections to be re-counted, and the results of recounts no doubt inform the public about the quality of vote counting overall.

As a result, voters trust election returns even in the absence of auditing. In the 2016 Survey of the Performance of American Elections, for instance, 91% of respondents from states that required no post-election audits at all stated that they were very confident or somewhat confident that their votes were counted as cast. This contrasts with 90% of respondents from states that required post-election audits. Even without formal audits, voters already express a high level of confidence that votes are counted accurately.

As to the promise that most sophisticated, mathematically rigorous techniques will convince candidates and the public of the veracity of election returns, one only need remember the notoriously poor level of "numeracy" that besets the American public. Even among the numerically sophisticated, understanding how risk-limiting audits work requires a level of statistical knowledge few people possess. As a result, adopting risk-limiting audits risks asking the public to shift blind trust from election officials to statisticians, which, in this age of skepticism about elite expertise, would seem to be a non-starter.[19]

The answer to this conundrum lies in the middle. Even trustworthy individuals make mistakes, and at the very least, rigorous auditing regimes can protect against those mistakes. Beyond this minimalist justification for pursuing better auditing methods, we should remember that some of the most critical electoral crises in recent memory have occurred due to problems that were flying below the radar, unnoticed by the public. The fact that the public at large does not appear to be overly alarmed at the quality of vote-counting does not mean that quality controls are currently adequate.

At the same time, proponents of more sophisticated measures, such as risk-limiting audits, have work to do in explaining how their procedures work and why the public should trust them. At the Summit, the par-

[19] The Summit presentation of William Kresse, cited above, provides further insights into the need to make RLAs "judge-friendly" and "media-friendly."

ticipants took part in an hour-long simulation of a ballot-polling RLA. As the exercise proceeded, it was clear that many of the participants failed to grasp the instructions and got lost in the process. This was a palpable sense to many in the room that moving RLAs from being the preferred method of auditing among the in-the-know experts to being widely accepted among regular citizens still has a long way to go.

HOW OFTEN ARE AUDITS NEEDED?

An important and overlooked issue in the movement toward more and more sophisticated post-election tabulation audits is the question of which elections to audit, and how frequently to audit them. As William Kresse noted in the final panel of the Summit, financial audits do not always cover the same material, nor at the same level of detail every time.

Is there something to be learned in the election auditing realm? Certainly, returns for high-visibility offices, such as U.S. president and state governors, should be subjected to risk-limiting audits every time. But, should every school board race or state legislative seat be equally scrutinized every time? This is where the American "long ballot" raises practical issues regarding post-election tabulation audits. As states become comfortable with risk-limiting audits and anticipate expanding them down the ballot, an important topic to consider is which down-ballot races should be audited, at what frequency, and chosen based on what process?

Furthermore, as already noted, tabulation is not the only election administration detail that should be subjected to auditing and other quality control procedures. How often should an audit of district assignments, of the sort discussed by Michael McDonald, be conducted, for instance?

HOW DO WE GET STATES AND COUNTIES TO IMPLEMENT ELECTION AUDITS? (THE HERE-TO-THERE PROBLEM)

Expanding the prevalence of auditing is a goal shared by a wide variety of election reformers and election administrators. The auditing culture has certainly expanded over the past decade. In 2008, fewer than half of the states, 23, required any sort of post-election tabulation audit. By 2016, that number had grown to 34, plus the District of Columbia.[20]

Of course, with only 34 states currently requiring any sort of post-election tabulation audit, and only three states requiring RLAs, there is still a long way to go before RLAs become ubiquitous.

It is clear that the expansion of election auditing will most likely be a state-by-state affair. Recent legislation introduced in both the House and Senate would mandate that all federal elections include post-election auditing. However, the legislation has stalled, over White House opposition and conflict over states' rights issues. At the same time, concern over cyber threats has caused states without auditing requirements to consider them, and for states with those requirements to investigate strengthening them.

Three of the chapters in this report, by Neal McBurnett, Hilary Rudy, and Jay Bagga and Bryan Byers, provide insights into how RLAs might be expanded, based on observations from one state that has already implemented them (Colorado) and from another state that is exploring the issue (Indiana).

[20] https://elections.mit.edu/#indicatorProfile-PEAR.

Colorado's experience lays out one blueprint for how RLAs might be rolled out on a statewide basis. Colorado, which first implemented statewide RLAs for the election in 2017 (which included local, municipal, and special district elections), has been the pioneer in the field. One factor that aided Colorado's embrace of RLAs is that it was integrated into a transformation of the voting model altogether, to a "vote-at-home" system, where ballots are mailed to all residents and they are then returned either by mail or at official locations.

In transitioning to the new system, Colorado was able to integrate the purchase of new voting equipment into the new auditing regime. With the vote-at-home model relying on the central counting of ballots, the record-keeping load on administrators was made manageable. The wholesale changeover to a new voting model also provided an opportunity to engage a variety of stakeholders into rethinking the election workflow, not just to facilitate RLAs, but also to improve administration overall.

Colorado still has challenges to surmount before the RLA path is completely smooth. Colorado has learned that implementing RLAs is software-intensive, and that the software doesn't write itself. It is still considering how to expand auditing beyond the top-of-the-ticket races. Much work still needs to be done.

(On the issue of software for RLAs, this is yet another example of how the implementation of a common data format for election returns, cast-vote records, and the like is needed to implemented critical reforms in election administration.)

Because of the enormous heterogeneity in terms of size, scope, and timing of elections in the United States, there is unlikely to be a one-size-fits-all auditing system for the entire nation, or even for local jurisdictions within states. The Summit heard examples of pilot projects in Colorado, New Jersey, California, Rhode Island, and Indiana that seemed to be successful in giving state and local officials information about how RLAs might be adapted to their own settings, and getting them comfortable with the ideas overall.

Although the purpose of conducting rigorous election audits is to assure the public that an election was conducted accurately, as well as to provide convincing evidence to losers that they in fact lost, the critical stakeholder in determining whether a state mandates audits, and whether those audits are rigorous, is local election officials.

Local election officials bear most of the administrative burden of implementing election audits, especially post-election tabulation audits. The typical local election office is small and runs on a tight budget. Anything that increases work without an obvious benefit to local officials will be met with howls of opposition from these local officials who, by the nature of their job, have the ears of those officials.

Bringing local officials on board to advocate for rigorous post-election tabulation audits requires more than simply explaining how they are done and why they are important. Showing how they are done, through the pilots mentioned earlier, seems to be one mechanism for opening up local officials to the feasibility of audits.

To the degree that explanation is important, one factor seems to trump all others: Under most circumstances, once the requisite systems are in place, RLAs require

less work after the election than do traditional fixed-percentage audits. With most elections decided by comfortable margins, RLAs will often require only the examination of a few hundred ballots in most cases.

Even when elections are close, the number of ballots examined under RLAs will likely be less than the number examined under more traditional methods.

WHAT CAN AMERICANS LEARN ABOUT AUDITING FROM OTHER COUNTRIES?

The attention paid to post-election auditing in the United States has tended to focus entirely on American elections, despite the fact that assessing the veracity of elections has long been a major issue in the administration of elections in other countries, as well as an important subject of scholarship. Observation of elections by international observers, such as the Organization for Security and Cooperation in Europe (OSCE), has been regarded as an important element in reducing corruption in countries that are considered problematic.

One challenge that auditing has to face in the developing world is that of sovereignty. Developing nations, trying to come out under centuries of colonial control, are keen to develop their own election apparatuses. This puts a premium on countries doing their own in-house audits. At the same time, lack of capacity often leads these countries to rely on international experts to supply statistical expertise.

Political scientists have piggy-backed their research on top of these efforts, to develop rigorous techniques to document how election-observation regimes can reduce corruption.[21] Many of these efforts can be grouped under the heading of "election forensics."[22]

In both her presentation to the Summit and her essay in this report, Emily Beaulieu, a leading scholar of international election observation and corruption, offered both optimistic and cautionary observations about election auditing internationally.[23]

The 2010 election in Haiti is one success story, where scrutiny of precincts with above-average (and in some cases, above-100%) turnout overturned the results of the preliminary election ended up with a result in which the original third-place finisher in the preliminary was allowed to go into the final round, ultimately winning. On the other hand, recent experience in elections in Afghanistan, Honduras, and Kosovo illustrate how audits alone can be insufficient to ensure that clear evidence of elections being stolen by fraud will result in new elections being demands, or consequences being felt for the perpetrators.

Whether these comments apply directly to the American case can be questioned. However, one point made by Beaulieu does seem applicable: Using audits to detect and correct election fraud will be more effect if citizens already have trust in elections. If they do not, then the results of audits will

[21] R. Michael Alvarez, Thad E. Hall, and Susan D. Hyde, eds. *Election fraud: detecting and deterring electoral manipulation*, Washington: Brookings, 2009.

[22] Allen Hicken and Walter R. Mebane Jr., "A guide to election forensics," USAID Research and Innovation Grants Working Paper Series, July 28, 2017, https://pdf.usaid.gov/pdf_docs/PA00MXR7.pdf.

[23] Beaulieu's presentation may be found at 40:55 of the conference video: https://youtu.be/kY5siXs-gWUI?t=2455.

become just another source of conflict over which competing political factions compete. At its worst, audits have the potential to deepen suspicious and cause a decline in voter confidence.

The techniques discuss by Walter Mebane have been applied to both American and non-American elections.[24] Unlike the techniques based on election observation, Mebane's methods primarily rest on the analysis of aggregate election data, matching that data against comparison statistics, such as turnout data, previous election results, and demographic data.

Mebane's presentation and essay return us to the point that all methods of auditing do not have to rest on an examination of individual ballots, as proposed by RLAs. Certainly, ballot-based audit methods are statistically superior to other methods, but ballots are not always available. In those cases, less powerful methods may be powerful enough to convince the public, local election authorities, and/or the international community that something was amiss in a nation's election.

NEXT STEPS AND MOVING FORWARD

The conference was a success, especially as it brought election officials, academics, and other stakeholders in election auditing together for two days of productive conversation and interaction. In a number of cases, conversations between academics and election officials, begun at the conference, have sparked subsequent conversations and perhaps even eventual collaborations.

We would like to see more collaborations between election officials and academics on election auditing, and to that end, we will start by proposing that convenings like this conference be held more regularly.

> *There is a strong and pressing need to continue to build trust and communication between election officials and academic researchers, in particularly when it comes to election auditing.*

There is a growing interest among academics in different areas of the election auditing process, and facilitating that interest by keeping academics in contact with election officials is important. Many election officials are interested in post-election ballot audits and comprehensive election auditing, but lack the time and statistical expertise to implement election audits on their own, so giving them the opportunity to connect with academics who might help them is important.

There is also a need to continue to facilitate the scientific study of election administration and technology, in particular as it relates to election auditing. The academics interested in election auditing have made significant progress in recent years developing auditing techniques and tools to perform different types of election audits. However, the research initiatives often exist within academic disciplines, and there is a need for more interdisciplinary communication about election auditing. So we also believe that there should be periodic workshops and conferences for the academics interested in studying election audits and integrity, which will help grown and strengthen scientific knowledge of auditing practices and methodologies.

[24] Mebane's presentation may be found at 14:23 of the conference video: https://youtu.be/kY5siXs-gWUI?t=863.

CURRENT STATUS OF POST-ELECTION AUDITING AND RECOUNT PRACTICES

RISK-LIMITING AUDITS AND EVIDENCE-BASED ELECTIONS

PHILIP B. STARK
University of California, Berkeley

No way of counting votes is perfect. Every system—manual or electronic—can make mistakes. Electronic systems are particularly vulnerable to misconfiguration, bugs, hacking, data loss, etc.

If there is a trustworthy paper record of voter intent, reported outcomes can be checked against that paper trail by suitable audits. But an audit is no better than the paper trail is relies on. If there is no paper trail, there is no way to verify whether the reported results are correct. If the paper trail is not voter-verifiable (e.g., the paper record produced by some ballot-marking devices), an audit cannot verify who won. If the paper trail is not trustworthy, the audited outcome is not trustworthy.

The key elements for ensuring reported election outcomes are trustworthy can be summarized with *"5 Cs"*:

- ***Create*** durable, trustworthy record of voter intent. Hand-marked paper ballots are best for voters who have the dexterity and visual acuity to use them; ballot-marking devices (BMDs) are helpful for voters with disabilities that make it difficult or impossible to mark a ballot by hand.[1]
- ***Care*** for the paper record. The chain of custody should be verifiable; there should be two-person custody rules, ballot accounting, good seal protocols, etc.
- ***Compliance*** audit. Auditors need to establish whether paper trail is trustworthy, through ballot accounting, checking against pollbooks and voter registration databases, reviewing chain of custody logs, video security surveillance, checking eligibility determina-

[1] See, e.g., https://www.stat.berkeley.edu/~stark/Preprints/bmd19.pdf

tions, checking signature verification, etc.

» ***Check*** reported outcome against the paper (using a risk-limiting audit).

» ***Correct*** the reported outcome if it is wrong (by conducting a full hand count).

A risk-limiting audit (RLA) is any procedure such that:

> *If an accurate full hand count of the paper would find different winners than were reported, the procedure has a known minimum chance of requiring a full hand count.*

The ***risk limit*** of a RLA is the largest possible chance that, if the reported outcome is wrong, the audit won't correct it. Here, ***outcome*** means the electoral outcome: the winner or winners, not the exact vote tallies.[2]

Many state audit laws go into great detail to specify how many ballots (or precincts) to audit. That focus is misplaced, in my opinion: the starting sample size is not important. What matters is when you *stop* auditing.

A RLA does not stop auditing until and unless there is strong statistical evidence that a full hand count would simply confirm the reported outcome—that it would be a waste of time. If it does not find strong evidence that the reported outcome is correct, a RLA progresses to a full hand count to set the record straight. If the outcome is wrong but the paper trail is trustworthy, a RLA has a known minimum chance of correcting the outcome. RLAs do not involve assumptions about voter preferences, nor about how or why errors might occur.[3]

Risk-limiting audits can be used with a broad variety of approaches to drawing random samples of ballots or groups of ballots, allowing audits to be tailored to the logistics and equipment of individual jurisdictions. The ***sampling unit*** can be a group of ballots or an individual ballot. The sample can be ***stratified*** or ***unstratified***. The sampling units can be drawn with equal probability, or with different probabilities (for instance, sampling with probability proportional to an error bound is useful when the sampling unit is a group of ballots). The sample can be drawn with replacement, without replacement, by Bernoulli sampling, by Poisson sampling, or many other methods.

Once the sample is collected, there are two main approaches to analyzing the data to determine whether the audit can stop. ***Poll-***

[2] In general, it is impossible to get the tallies right to the last vote without a full, accurate hand count. But getting the electoral outcome right seems like the minimal acceptable standard. If we do not audit enough to determine with high confidence who won, we are not auditing enough.

[3] Bayesian audits are not, in general, risk-limiting audits. Bayesian audits assume voter preferences are random, with a known distribution. They answer the question, "if the current election had been selected at random from a particular hypothetical population of elections, then, given the audit data, what is the probability that the current election is one of those hypothetical elections for which the reported result is correct?" The "upset probability" for a Bayesian audit is in general much smaller than the risk that a Bayesian audit will not correct the outcome if the outcome is wrong. There are examples where the "upset probability" is 5 percent, but there is a 55 percent chance that the Bayesian audit will not correct a wrong outcome.

RLAs and Bayesian audits both require a trustworthy paper trail, random sampling, etc. The biggest operational difference between them is the rule for deciding whether the audit can stop—but they answer very different questions. In particular, a Bayesian audit might not have a large chance of correcting the outcome if the outcome is wrong.

ing audits use the audit data directly. They are like exit polls, but instead of asking voters how they voted, they get that information directly from the ballots. Unlike voters, ballots have to reply (and have to reply honestly). The only information a polling audit needs from the voting system is the reported winner(s).

Comparison audits use the audit data together with detailed information exported from the voting system. They compare how the equipment tabulated randomly selected ballots with how humans would tabulate the same ballots. Comparison audits are like checking someone's reported travel expenses: First, add up the reported expenses to check the math. Second, spot check the reported expenses against the underlying paper receipts to make sure the expenses were reported accurately.

Similarly, a comparison audit starts with data exported from the voting system: vote subtotals for individual ballots or groups of ballots. First, auditors check that the reported subtotals add up to give the overall reported results. Second, auditors draw ballots or groups at random and manually check whether the reported subtotals were correct. If the audit finds convincing evidence that the tabulation was accurate enough that the reported winner must have won, the audit can stop.

Any jurisdiction that uses paper ballots (and keeps track of the ballots) can perform a ***ballot-polling risk limiting audit***; no special voting equipment is needed. However, the efficiency of the audit—measured by the number of ballots that must be inspected before the audit can stop—does depend on the capabilities of the voting system. If the voting system can report how it interpreted individual ballots (i.e., if it can report a cast-vote record for each ballot) in such a way that the corresponding physical ballot can be identified and retrieved for manual inspection, then a ballot-level comparison audit is possible. When the reported electoral outcome is correct, ballot-level comparison RLAs generally require inspecting far fewer ballots than ballot-polling RLAs, especially when the margin is small.

COMPREHENSIVE ELECTION PERFORMANCE AUDITING

R. MICHAEL ALVAREZ
California Institute of Technology

Over the last two decades, the technology and administration of American elections have become hot topics in public discourse. No longer is the conduct of elections a matter of discussion among a small group of academics, nor is it a relatively obscure area of state and local public administration. Discussions about the integrity of recent elections have dominated headlines and been central topics of debate in the 2016 presidential and 2018 midterm elections. From allegations of cyber-attacks on election administration and database systems in recent years, to debates about election malfeasance in some states, there is more discussion of election security and integrity than ever before.

Given the public focus on the integrity of elections, the question that continues to arise is how does the public know that an election has been conducted with a high degree of integrity? How can we be sure that there weren't successful attempts to hack voter registration databases, to stuff ballot boxes, or to impersonate vote-by-mail voters? Furthermore, how can we confirm that proper procedures were followed in all vote centers and polling places, that voter rights were maintained, and that in the end, all ballots were counted as intended? Confirming the integrity of an election is no simple matter.

In the past, many election jurisdictions used certain forms of auditing approaches to attempt confirmation that aspects of their election process and voting systems were functioning as expected. For example, in many jurisdictions, pre-election "logic and accuracy" tests have been conducted on sampled voting machines to ensure that they record votes as they should, and in some states, certain types of post-elec-

tion ballot audits are used to provide some assurance that ballot recording and tabulation may have functioned as expected in an election. States and counties continue to improve and innovate with respect to these practices, for example, by testing and implementing "risk-limiting audits." These newer forms of post-election auditing can provide statistical confirmation that ballots were tabulated correctly.

These types of auditing procedures are important. But they only can help to assess the integrity of some aspects of election administration. For example, a ***"logic and accuracy"*** test of voting equipment used for in-person ballot marking on Election Day or in a vote center doesn't shed any light on the integrity of a jurisdiction's voting-by-mail process, nor does a post-election ballot audit help us determine the integrity or accuracy of a jurisdiction's voter registration process and databases.

> *For a more complete assessment of the integrity of an election in a state or county, we need different and more comprehensive methodologies that can evaluate the performance of the entire election jurisdiction's "eco-system."*

In addition, the analyses that serve as the justification for that assessment should be transparent and available to the public.

Working in collaboration with the Orange County Registrar of Voters (OCROV), Neal Kelley, and his team, our research group at Caltech pilot-tested an ambitious set of comprehensive election performance auditing methodologies in the 2018 primary and general elections in Orange County. In our pilot project, we wanted to develop and deploy auditing and performance measurement tools that would be both relevant and actionable for the OCROV, as well as timely and transparent for stakeholders and the public. We also sought, as much as possible, to focus on election performance data that were already being generated by OCROV ("trace data") or on data that we could produce and analyze independently of OCROV; this strategy would minimize the amount of time and resources that OCROV needed to devote to this pilot project in the course of a busy and complex election cycle, while also producing an independent evaluation of the administration of the 2018 primary and general elections in Orange County, California.

Orange County was chosen because it is an ideal location for a pilot project like this. First off, the OCROV and his team have an established record as innovators, and prior to our collaboration were already generating a great deal of data. Secondly, election administration in California is changing rapidly; for example, in 2020 Orange County will be moving away from the traditional neighborhood voting model towards universal vote-by-mail and voting centers; starting our pilot project in 2018 in Orange County provided an important baseline for longitudinal analysis of these changes and their potential implications for voter confidence. Third, Orange County is a large (approximately 1.5 million active registered voters) and diverse election jurisdiction in Southern California. Finally, in 2018 we expected to see many hotly contested elections, in particular for U.S. House seats in Orange County—helping us gauge which performance measures might be more relevant and important in competitive elections.

For both the 2018 primary and general elections in Orange County, we built and implemented a number of different performance methodologies:

1. mail ballot transmission and return tracker;
2. in-person observation studies of early and Election Day voting;
3. post-election precinct-level turnout and candidate forensics and anomaly detection analytics;
4. post-election voter surveys (general election);
5. voter registration auditing;
6. observation and study of OCROV's post-election risk limiting audits; and
7. social media monitoring.

Reports and summaries of these election performance methodologies for both election cycles are available on the project's website (https://monitoringtheelection.us).

Our 2018 Orange County comprehensive election performance auditing project has yielded a great deal of important analytical data, and a number of conclusions for our continued research on developing this approach for providing a data-driven evaluation of election integrity.

First, of the methodologies that we developed and deployed in 2018, we believe that the most useful for election officials is our voter registration auditing methodology: we developed an approach that flags anomalous changes in the voter registration data for further investigation. Second, producing timely and actionable performance measurement is crucial for both election administrators and the public; during the immediate post-election canvass period is when concerns about election integrity arise, and it is imperative for maintaining voter confidence that performance measures and analyses be up-to-date and available to the public in the days and weeks following Election Day. Third, some of our methodologies, like social media monitoring and turnout/candidate vote share forensics, have considerable promise as election performance tools, but they require continued research and further development. Finally, and most crucially, the 2018 election cycle in Orange County was quite competitive—our comprehensive election performance audit provided substantial data-driven evidence that these elections were administered with integrity, and that voters should be confident that their votes were tabulated as they intended.

Looking forward, our research group will continue to test, develop, and implement the methodologies used in 2018 in Orange County in future elections. Our immediate plan is to scale our comprehensive election performance auditing approach to cover Southern California in the 2020 presidential election cycle. By adding additional counties, we will build important variance in context that will give us greater opportunity to compare performance across jurisdictions within the same state. This will also move us closer to being able to deploy comprehensive election performance auditing for most American states (covering Orange and Los Angeles Counties in 2020, for example, would include approximately 7 million registered voters in our analysis, a greater population of registered voters than in all but the largest American states. And this will give us important longitudinal data for Orange County, which we can use to track election integrity over time.

ELECTION VALIDATION PROJECT

INCREASING TRUST IN ELECTIONS THROUGH AUDITS, STANDARDS, AND TESTING

JENNIFER MORRELL
Democracy Fund

This is a unique time in election administration. Never before have there been so many resources, tools, and information for election administrators. In fact, towards the end of my time as a local election official, I felt overwhelmed by all of the ideas and information pouring in. I could not keep up with reading it all, let alone implementing it.

A serious discussion about the role that election audit standards might play in validating our elections must also include a discussion about strategies for taking an idea as broad as audits and creating something that will actually be read and used by state and local election officials. One way to start is by clearing away the clutter.

Think about the strategy you would follow to teach someone a new skill, such as baking a loaf of bread. You would not start by asking them to read all of the literature ever written about bread making. You start by forming a basic understanding of the important principles. Next you demonstrate what tools are available, which ones are necessary and which ones are optional but might make the task easier, followed by providing a recipe or guidelines that include the necessary ingredients and instructions. Finally, you have someone with experience demonstrate how the process works and act as a mentor.

We can do the same for risk-limiting audits by providing a practical guide for state and local election officials that covers the following:

- Terms and definitions
- Policy considerations
- Voting equipment and technology
- Implementation considerations

Implementing RLAs becomes more likely when practical guidelines are coupled with templates for ballot organization and storage, pilot audits to provide hands on experience, auditing software, and pairing up states who are or plan to conduct risk-limiting audits to help mentor each other.

It is also important to recognize the gaps that need to be addressed before a concerted push is made for wide-spread implementation. With respect to post-election, risk-limiting audits, there is a need to create better communication about the process, a universal audit tool or software to assist with the audit, better ways to retrieve ballots (especially for ballots scanned at the polling location), ways to ensure the audit material does not compromise voter anonymity, and deciding if it is appropriate to create national standards. These are all areas where outside organizations can contribute possible solutions.

Not every state may be able to or have a desire to implement risk-limiting audits. Resistance to change is universal and there may be reasons to make a careful and gradual move towards risk-limiting audits. It does not need to be an immediate destination but can be viewed more as a path with steps leading to it. Some steps that will help ease the transition toward RLAs:

- Strong collaboration among state and local election officials
- Making the RLA terms and definitions a regular part of election vocabulary
- Creating documented voter intent guidelines
- Developing a well-crafted plan for ballot storage and organization
- Requiring precise ballot reconciliation
- Implementing dates and deadlines to accommodate time for a post-election audit prior to certification
- Basing the number of ballots selected for audit on the contest margins
- Using dice or similar method to randomly select the ballots, precincts, voting machines, etc. that will be audited
- Purchasing a voting system that produces a voter verifiable paper ballot and cast vote record

Most of the focus has been on robust, post-election audit of the vote tabulation equipment, such as risk-limiting audits. But it begs the question why only audit and test the voting equipment? Why not audit and validate other critical components of the election system? Auditing how votes are tabulated plays an important role in validating the outcome of an election. However, it is only one of several elements in the election system that needs to be examined.

A risk-limiting audit provides modest benefit if you cannot provide evidence of a solid chain of custody from the beginning of an election to the end, for both ballots and voting equipment.

As we start to think about incorporating audit principles into election administration, consider other critical components in the election system that can be audited:

- Voter registration databases
- Voter district and precinct assignments
- Security procedures (physical and cybersecurity)
- Pre-election testing of voting equipment (focused on paper ballots)
- Ballot reconciliation and chain of custody

- Ballot layout and design
- Resource planning and allocation (enough equipment, supplies, and people to meet demand)

State and local election offices increasingly employ or contract with a number of experts. This includes individuals with a professional background or expertise in law, communications, data analysis, project management, and cybersecurity. It may be time to consider including auditing and quality control professionals into that mix.

Audits have played a role in U.S. companies for many years. Many of those same auditing standards and definitions can be applied to elections. For instance, an audit can be defined as a systematic, independent and documented process for obtaining audit evidence and evaluating the evidence objectively to determine the extent to which the audit criteria are fulfilled.

We can also apply standard classifications for the type of audit being performed. A ***product audit*** is the examination of a particular product (such as a voting system) to evaluate whether it conforms to requirements and performance standards. A ***process audit*** evaluates an operation against predetermined instructions or standards and asks the questions: *Did the operation conform to the standards? Are the instructions for the operation effective?* The audit typically examines resources (equipment, materials, people), environment, and methods (procedures and instructions).

A ***system audit*** verifies that applicable elements of the system are appropriate and effective and have been developed, documented, and implemented in accordance with specified requirements. For example, an election system audit would determine if the election system conforms to state and federal policies and requirements.

When an election audit is implemented the standard phases of an audit are also applicable and include:

1. preparation;
2. conducting the audit;
3. reporting and feedback; and
4. closure.

Most of the workload that will fall to local election officials is in the preparation stage.

Audits can be both internal and external. In an internal, or ***first-party audit***, an organization measures its strengths and weaknesses against its own procedures or against external standards. In an external, or ***third-party audit***, the audit is performed by an independent audit organization and free of any conflict of interest.

We can also apply the benefits of conducting an audit to elections:

- Detects voting system errors
- Provides accountability to voters
- Deters fraudulent activity
- Limits the risk of certifying incorrect outcome
- Assures votes were counted & reported accurately
- Provides feedback for process improvement

We are at our best when we face complex challenges together.

We no longer have the luxury of working in our individual silos. The solutions to successfully planning for, conducting, and auditing an election will come from a diversity of professional backgrounds collaborating on research and exploring new ideas. This includes thinking about how technology and solutions already employed in other sectors can be used to improve election administration. We need each other—election officials, technology experts, academics, policy makers and election advocacy groups—all working together to build public trust in elections.

POST-ELECTION AUDITS: THE STATE OF THE STATES

DYLAN LYNCH
National Conference of State Legislatures

Much of what we do at the National Conference of State Legislatures is group and categorize state policies to provide a national overview. This allows state legislators and others to easily compare policies across the country. For post-election audits we have organized state policies into three general categories.

AUDIT TYPES ACROSS THE COUNTRY

1. Traditional. Traditional audits look at a fixed percentage of voting districts or voting machines and compare the paper record to the results produced by the voting system. Regardless of the closeness of a race, they will always count the same number of ballots. Although the way these states conduct audits is similar, differences do exist. For example:

- *What is counted:* In Alaska, a randomly selected precinct in each house race is selected and 5 percent of ballots cast in the district are audited. In Nevada, the audit looks at 2 percent or 3 percent of voting machines, depending on county size.
- *Who conducts the audits:* In New Mexico, an independent auditor in hired by the secretary of state (SOS) and oversees the audit. In Pennsylvania, the local boards of elections do it. And in Vermont, the SOS conducts the audit.
- *When is the audit conducted:* In Florida, the audit is conducted following the certification of election results while Illinois conducts theirs before the canvassing of ballots.

2. Risk-limiting audits (RLAs). By their simplest definition, RLAs are "statically based audit techniques." Washington's Revised Code §29A.60.185(c) further defines and explains a risk-limiting audit as:

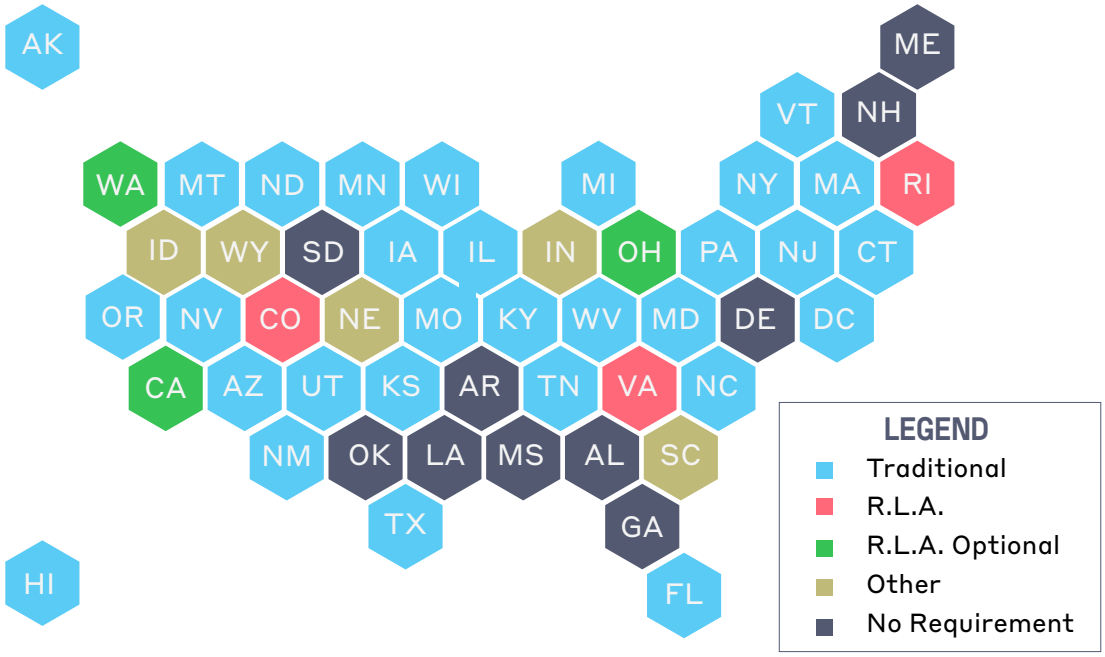
c) A risk-limiting audit. A "risk-limiting audit" means an audit protocol that makes use of statistical principles and methods and is designed to limit the risk of certifying an incorrect election outcome. The secretary of state shall:

(i) Set the risk limit. A "risk limit" means the largest statistical probability that an incorrect reported tabulation outcome is not detected in a risk-limiting audit;

(ii) Randomly select for audit at least one statewide contest, and for each county at least one ballot contest other than the selected statewide contest. The county auditor shall randomly select a ballot contest for audit if in any particular election there is no statewide contest; and

(iii) Establish procedures for implementation of risk-limiting audits, including random selection of the audit sample, determination of audit size, and procedures for a comparison risk-limiting audit and ballot polling risk-limiting audit as defined in (c)(iii)(A) and (B) of this subsection.

Only three states have enacted RLAs in statute and only Colorado has fully implemented a statewide RLA. However, many other pilot programs, generally done at the local level, have been completed across the country. In addition, three states are currently in the process of phasing-in RLAs (California), or allowing local jurisdictions the option of conducting a RLA, (Ohio and



Washington). More details about these states can be found below.

3. "Other." This, again, can vary. In some states, like Idaho, an audit is triggered only when a recount is required. Some states have a procedural audit, which is not necessarily an audit of ballots, but is instead an audit of the processes and procedures used in the election.

As the map on the previous page shows, traditional audits are by far the most common route states take, with a smattering of states that use RLAs and "other" types of audits. However, a few interesting things are going on in some states. New Mexico and Oregon are categorized as traditional audits, but really enact a tiered system.

In a tiered system, the margin of victory of a race dictates how many ballots are audited. The closer the race, the more ballots that get audited. Meanwhile, in September 2018, California passed Assembly Bill 2125, which stipulated that in lieu of the traditional audit, beginning with the spring primary of 2020, a county can choose to conduct a risk limiting audit. In addition, Ohio and Washington have "optional" R.L.A.s. In Ohio, a 2017 directive from the secretary of state recommended RLAs be used by counties but did not mandate them. In Washington, county auditors can choose among three post-election audits methods, with an RLA being one of the three.

Lastly, there was a decent amount of auditing action taken in Michigan in 2018. During the 2018 general election, the state ran an RLA pilot program in three cities. In addition, on the ballot in that election was Ballot Measure 18-3, a proposed state constitutional amendment that would have established many election policies, including a post-election audit, as rights in the state constitution. The measure passed, and the legislature enacted a traditional post-election policy in late December 2018.

YEAR	STATES WITH BILLS	BILLS INTRODUCED	BILLS ENACTED
2011	10	16	2
2012	9	14	2
2013	10	14	0
2014	11	21	4
2015	10	18	0
2016	10	22	2
2017	16	23	4
2018	21	48	10
TOTAL		**176**	**24**

LEGISLATION

Moving on to state legislation, post-election audits have been a topic throughout the states for many years. Starting in 2011, there was a consistent number of bills until an increase in 2016.

In total from 2011 to 2018, 176 post-election audit bills were introduced, with only 24 being enacted.

TOPICS FOR CONSIDERATION

Risk-limiting audits have certainly gained traction not only in legislatures, but also in the media. Yet, there are some things that may need consideration or discussion if state legislatures want to enact RLAs.

The Good:

- ***Implementable.*** We know that RLAs are possible. Colorado put in a lot of the legwork, but if other states look to implement RLAs, the process could become more streamlined and efficient.
- ***Integrity, Security and Confidence.*** RLAs provide integrity, security and confidence to the outcome of an election. Confidence in the democratic system is vital to the maintenance of our system governance.
- ***Cost/Time Savings.*** RLAs, as a system, could provide cost and time savings compared to traditional audits

The Bad:

- ***Not Everyone is Ready.*** Not every state is ready for RLAs. Colorado did put in a lot of work and time and money into their effort. Not every state can do so at this time.
- ***Technology Considerations.*** Many states may not have the equipment or technology necessary to efficiently conduct an RLA.
- ***Initial Time/Cost.*** Because this is somewhat unchartered territory, states may need to put a lot of initial work into creating a system that works with their structure and adheres to their laws.

The Ugly:

- ***Legislation for the Sake of Legislation.*** Many would agree that legislation should be based on informed decision making. Passing legislation just to have it in the books can lead to legislative and administrative issues that could ultimately sink the policy if a state is not ready.
- ***Complexity.*** If you asked the average voter if they wanted to learn about "statistically based audit techniques," how do you imagine that going? Because the point of RLAs is to provide confidence and security, that requires everyone having a basic understanding of the how and why. What is probably most detrimental to RLAs is the public believing RLAs operate like "magic".

CONCLUSIONS

Post-election audits aren't going away. In fact, audits are increasingly spreading into other areas of election administration, such as voter registration logs, voting equipment and other election procedures. It is possible that elections are becoming more audit centric. Still, we are fond of calling states "the laboratories of democracy" and as such, states will continue to make policy decisions that work for and suit them best.

NEW STATISTICAL APPROACHES TO AUDITING VOTE TABULATION AND RECOUNTS

SAMPLING WITH *K*-CUT, AND BAYESIAN AUDITS

RONALD L. RIVEST
Massachusetts Institute of Technology

INTRODUCTION

We present two new tools for the election auditor's toolbox that may provide increased efficiency, or additional flexibility in complicated situations.

Post-election statistical tabulation audits proceed by sampling cast paper ballots at random, and then figuring out what the sampled ballots tell you about the correctness of the reported election outcomes.

We propose a new procedure, ***sampling with k-cuts***, for drawing random samples of cast paper ballots for such statistical post-election audits. This procedure eliminates the need to count down to a specified pseudo-random position in a stack of ballots, by performing instead a sequence of ***k "cuts"*** (like cutting a deck of cards) and then taking the top ballot. Sampling with *k*-cuts works well with ballot-polling audits, but doesn't work at all for ballot-comparison audits (which need to find a ballot with a specified imprinted ballot ID).

We also propose the use of ***Bayesian audits*** for determining whether to accept the reported election outcome or to continue the audit (by examining a larger sample). Bayesian audits are an alternative to "***risk-limiting audits***," and are of particular interest when no risk-limiting audit method is available or feasible.

SAMPLING WITH *K*-CUT

> *How can one pick a ballot "at random" from a given stack of ballots?*

The usual method is to generate a random ballot number (using cryptographic methods), and then to count down in the stack

to the ballot at that position. This method is tedious and error-prone when the stack is large.

Our proposed alternative, *k*-cut, works as follows to randomly sample a single ballot from a stack of ballots. (This procedure can be repeated to sample multiple ballots.)

- Pick a suitable small integer *k* (we suggest using $k = 6$).
- Perform *k* "cuts," where each cut removes a random fraction of ballots from the top of the stack and places those ballots at the bottom of the stack.
- Pick the ballot now at the top of the stack as your selected ballot.

Although each cut may individually be slightly non-uniform, repeating the operation *k* times smooths out the statistics to give acceptably uniform results.

A detailed analysis of the k-cut method appears in Mayuri Sridhar's Master's thesis,[1] and in Rivest and Sridhar, 2018.[2] Further research is underway to show how to improve (decrease) *k*, by making use of randomness "hints" when picking a cut size; decreasing *k* would provide further efficiency improvements.

The *k*-cut method has been used successfully in several pilot election audits (Indiana, Michigan, Rhode Island); going forward it is an attractive choice for use in actual (ballot-polling) audits.

[1] Mayuri Sridhar. Optimization for Election Tabulation Auditing. MIT EECS Master's Thesis. February 2019. https://mayuri95.github.io/main.pdf

[2] Mayuri Sridhar and Ronald L. Rivest. *k*-cut: A Simple Approximately-Uniform Method for Sampling Ballots in Post-Election Audits. Proceedings Financial Cryptography, February 2019, Fourth Workshop on Advances in Secure Voting. https://fc19.ifca.ai/voting/program.html

BAYESIAN TABULATION AUDITS

A ballot-level statistical post-election tabulation audit keeps drawing cast paper ballots and manually examining them, until it is determined that the sample drawn provides sufficient support for the reported outcome, or until all cast paper ballots have been examined.

There is more than one way to use statistical methods to define a "stopping rule" for the audit. "Risk-limiting audits" are one way; Bayesian audits are another (although there is some overlap).

A risk-limiting audit asks "What is the current risk if we stop the audit now?", and stops the audit if this risk is below a pre-defined ***risk limit***. Here risk is defined as the (conditional) probability that if the reported outcome is incorrect that the audit would accept the reported outcome as correct.

A Bayesian audit asks "What is the `upset probability'?"—the probability that examining all of the cast paper ballots would show the winner to be different than the reported outcome—and stops the audit if this upset probability is below a pre-defined ***upset probability limit***. Bayesian methods are used to define the upset probability as the posterior probability of an upset, given the sample and given a prior probability on ballots.

These definitions appear very close, but there are nonetheless significant differences.

For one thing, risk may be viewed as a worst-case definition, while upset probabilities are more of an average-case definition. Given the adversarial nature of elections, a risk-limiting audit may in general be a more

appropriate choice than a Bayesian audit (and we recommend using risk-limiting audits whenever possible).

Also, risk and upset probabilities appear not to be on the same scale: a risk-limit of five percent may correspond (roughly) to an upset probability limit of one-half of one percent or so (ten times smaller). Determining the relationship between risk and upset probability is an active research area. Achieving risk below a certain risk-limit is not the same thing as achieving an upset probability below a certain upset probability limit. One can't naively switch back and forth between the two models; the definitions mean different things.

Nonetheless, risk-limiting audits and Bayesian audits are ***highly compatible***. Their high-level structure is identical: drawing increasingly large samples until a stopping rule says to stop. A Bayesian audit can easily "piggy-back" on a risk-limiting audit, using the same sample data, and computing upset probabilities while the risk-limiting audit is computing risk. This can provide additional comfort and confirmation that the reported outcome is likely to be correct.

How does one implement a Bayesian audit? The following outline sketches one approach (based on "Polya's Urn") for computing an upset probability:

1. Draw an initial random sample of the cast paper ballots; examine each sampled ballot manually to determine the voter's intent.
2. "Pretend" to examine the remaining ballots, but instead of drawing new ballots randomly to examine manually, look at randomly chosen ***previously examined*** ballots again (with probability proportional to the number of times each ballot has been previously examined).
3. Compute the winner of the set of all (really drawn and pretend-drawn) ballots.
4. Repeat steps 2–3 many times. The fraction of time that the reported winner loses is the "upset probability."

The Bayesian audit stopping rule says to stop the audit if the estimated upset probability is below the pre-defined upset probability limit.

The Bayesian method is quite simple. One nice feature is that it works at the ballot-level, and is independent of the voting method used. The same approach works for plurality, approval voting, instant-runoff voting, etc. All that is needed is a method to determine the winner (step three above) for a set of ballots, and one must have such a procedure anyway just to run an election!

It should be noted that Bayesian methods require the definition and use of a "***prior probability distribution***" giving the assumed likelihood of seeing any particular ballot prior to seeing any sample data. In this use of Bayesian methods for post-election audits, defining such a prior is much easier than for many other applications of Bayesian methods, since the only purpose of the prior here is to ensure that a priori all ballot choices are judged equally likely.

The prior is weighted to ensure that it "steps out of the way" when the sample data arrives. In the above sketch, a typical prior would be effected by including one extra ballot for each candidate in the sample as part of step one.

One may also easily extend Bayesian methods to handle ballot-level comparison audits, or various forms of stratified audits (where some strata are ballot-polling and some are ballot-comparison).

Details omitted here; see Rivest[3] for an expanded treatment, and see the original Rivest and Shen[4] paper for more variations.

Bayesian methods have been implemented and used in various pilot audits; typically as a "free add-on" to a risk-limiting audit. For example, in the December 2018 pilot audit of a proposition on the ballot in Rochester Hills, Michigan, Kellie Ottoboni and Philip Stark computed (for a sample of 76 ballots with 50 Yes votes and 26 No votes) a risk of 2.1%, while Mayuri Sridhar computed an upset probability of 0.3%.

Again, these numbers are not directly comparable, but both are significantly below their pre-defined limits, so both the risk-limiting audit and the concurrent Bayesian audit (on the same sample data) confirmed the reported election outcome.[5] Bayesian audits have been used in a number of other pilot audits as well.

In summary, Bayesian methods provide additional tools in the auditor's arsenal, and may in some cases (for complex voting methods where no risk-limiting audit method is known) be the only tools available. For typical plurality elections, Bayesian methods are probably best as a possible concurrent "second opinion" on the correctness of the reported election outcome.

[3] Ronald L. Rivest. Bayesian Tabulation Audits: Explained and Extended. arXiv https://arxiv.org/abs/1801.00528 (2018-01-02)

[4] Ronald L. Rivest and Emily Shen. A Bayesian Method for Auditing Elections. Proceedings 2012 EVT/WOTE Conference. https://www.usenix.org/conference/evtwote12/workshop-program/presentation/rivest

[5] Scott Borling, Tina Barton, Chris Swope, Virginia Vander Roest, Mayuri Sridhar, Kellie Ottoboni, Liz Howard. Eds. Ron Rivest, Jerome Lovato, Philip Stark. A Review of Robust Post-Election Audits: Various Methods of Risk-Limiting Audits and Bayesian Audits. Brennan Center for Justice and Verified Voting. 2019 (to appear).

ELECTION FORENSICS BEYOND AUDITS

WALTER R. MEBANE, JR
University of Michigan

INTRODUCTION

Election forensics[1] can be useful in at least two circumstances: when effective audits are not feasible or even not possible; when problems going beyond what an audit may detect are suspected of affecting an election. I define election forensics as:

> *the use of statistical methods to determine whether the results of an election accurately reflect the intentions of the electors.*

Most audits use statistical methods, but the range of methods considered as included in election forensics is wider. Election forensics methods may focus on trying to provide evidence that an election outcome is correct, but they may also—or instead—focus on suggesting why election returns are as they are, pointing out anomalies, revealing possible fraudulent manipulations or intimidations, explaining outcomes as due to routine strategic behavior or identifying areas that should be investigated further using more richly informed hands-on methods.

Election forensics were first developed to apply in cases where paper records of votes are not available, so the question was whether anything at all could be done to create evidence regarding an election's

[1] Mebane, Jr., Walter R. 2008. Election Forensics: The Second-digit Benford's Law Test and Recent American Presidential Elections. *In The Art and Science of Studying Election Fraud: Detection, Prevention, and Consequences*, ed. R. Michael Alvarez, Thad E. Hall and Susan D. Hyde. Washington, DC: Brookings Institution.

credibility in such circumstances.[2] By now many have contributed methodologies, and productive scientific controversies and research abound.[3] Election forensics are very far from perfect. Indeed, it's best to think of them as nascent. For example, methods based on the second significant digits of vote counts have been shown to be ambiguous: they respond both to normal political activities (strategic behavior, district imbalances, special mobilizations, coalitions) and to frauds.[4] Methods that examine the last digit of vote counts can be fooled if malefactors have sufficient control over the numbers.[5]

In my presentation I briefly reviewed four recent applications of election forensics analysis and discussed one extension being developed to incorporate new kinds of data. The applications refer to some kinds of statistics that are available via the Election Forensics Toolkit (available at http:// election-forensics.ddns.net:3838/EFT_USAID) and some others.

HONDURAS 2017

Polling station data from the 2017 Presidential Election in Honduras shows signs of frauds that may have affected enough votes to determine the election outcome. One Toolkit indicator ("P05") suggests that votes for the winning party may have been manipulated. Estimates from a likelihood finite mixture model[6] suggests fraudulent vote counts are present in about thirteen percent of polling stations, and that the overall number of fraudulent votes is greater than the difference in votes between the winner and the second-place candidate.

US 2016 WISCONSIN AND MICHIGAN

Briefly reviewing results reported more completely in Mebane and Bernhard,[7] I describe evidence that the voting technologies used in places that had the votes recounted in these states appear to have treated candidates Trump and Clinton symmetrically. In Wisconsin, there was a full recount and in Michigan there was a partial recount. In Wisconsin a variety of methods were used to recount the ballots, including both hand

[2] Wand, Jonathan, Kenneth Shotts, Jasjeet S. Sekhon, Walter R. Mebane, Jr., Michael Herron and Henry E. Brady. 2001. "The Butterfly Did It: The Aberrant Vote for Buchanan in Palm Beach County, Florida." *American Political Science Review*

[3] e.g. Myagkov,. Ordeshook, and Shaikin in *The Forensics of Election Fraud: With Applications to Russia and Ukraine*; Levin, Cohn, Ordeshook, and Alvarez. in "Detecting Voter Fraud in an Electronic Voting Context: An Analysis of the Unlimited Reelection Vote in Venezuela;" Mebane, in"Fraud in the 2009 Presidential Election in Iran?;" Deckert, Myagkov, and Ordeshook in "Benford's Law and the Detection of Election Fraud;" Beber and Scacco in "What the Numbers Say: A Digit-Based Test for Election Fraud;" Klimek, Yegorov, Hanel; and Thurner in "Statistical Detection of Systematic Election Irregularities;" Mebane in "Election Forensics: Frauds Tests and Observation-level Frauds Probabilities;" and Ferrari, McAlister, and Mebane in "Developments in Positive Empirical Models of Election Frauds: Dimensions and Decisions."

[4] Mebane, Jr., Walter R. 2013a. "Using Vote Counts' Digits to Diagnose Strategies and Frauds: Russia;" and Mebane, Jr., Walter R. 2014. Can Votes Counts' Digits and Benford's Law Diagnose Elections? In *The Theory and Applications of Benford's Law*, ed. Steven J. Miller.

[5] Mebane, Jr., Walter R. 2013b. "Using Vote Counts' Digits to Diagnose Strategies and Frauds: Russia;" and Verena Mack and Lukas F. Stoetzer. 2019. "Election fraud, digit tests and how humans fabricate vote counts—An experimental approach." Electoral Studies 58(1):31–47.

[6] Mebane, Jr., Walter R. 2016. "Election Forensics: Frauds Tests and Observation-level Frauds Probabilities."

[7] Mebane, Jr., Walter R. and Matthew Bernhard. 2017. "Effects of Voting Technologies and Recount Methods on Votes in Wisconsin and Michigan;" and Mebane, Jr., Walter R. and Matthew Bernhard. 2018. "Voting Technologies, Recount Meth- ods and Votes in Wisconsin and Michigan in 2016.

and machine tabulations. In Michigan, all recounts were by hand. The diversity of voting and recount methods in the one case and incomplete coverage in the other makes it impossible say to anything with great confidence about whether voting machines were hacked in these states. Records from Wisconsin show that officials logged a variety of problems beyond "Voting machine error," and such errors were associated with some of the highest mean differences between the recounted and original vote count in Wisconsin wards.

KENYA 2017

Polling station data from the 2017 presidential election in Kenya produces extensive signs of frauds when analyzed using Toolkit methods.[8] This is the election that was annulled by the Kenyan Supreme Court. The most important challenge for election forensics analysis of Kenyan election data is that voting is very strongly polarized along ethnic lines. The strategic coordination around ethnicities creates patterns in vote count data that can look like frauds to statistical tests. The appearance of frauds is greatly reduced but not eliminated when the data are analyzed separately by county.

Unfortunately measures of ethnic composition are not available for Kenyan polling stations or other localities, but experts agree that many counties are ethnically much less heterogeneous than is the whole country. The analysis done separately by county still suggests there were many irregularities and thousands of fraudulent votes, possibly benefitting—in different counties—both leading candidates.

RUSSIA 2016

Polling station data from Russian national elections from 2000 through 2016 suggest that frauds in these election-type events have gotten worse over time.[9] A change appears to occur between the 2003 Duma and 2004 presidential elections: vote manipulations designed to "signal" that votes are being manipulated for United Russia are evident via the "P05" statistic from 2004 on. "P05" statistics suggests that turnout was being manipulated in all the elections. Estimates from the finite mixture model suggest the manipulations follow two basic patterns, with either substantial or very substantial proportions of votes being manufactured. While the "substantial" variant of the vote-manufacturing mechanism appears to have been in place during the 2016 presidential election, the proportion of polling stations in which frauds had effect is estimated to be the highest that year across all the elections. The number of fraudulent votes estimated to have been counted in that election dwarfs the other elections—the number is more than double the next highest estimated number of fraudulent votes.

TWITTER ELECTION OBSERVATORY

Based on 6.5 million keyword-filtered Tweets taken from the Streaming API, we used machine classification tools to extract 315,180 election incidents reported by 215,230 Twitter users during October 1–November 8, 2016: the initial implementation of a Twitter Election Observatory.[10]

An ***election incident*** is a report of a personal experience with situations such as lines

[8] Mebane, Jr., Walter R. 2017. "Anomalies and Frauds(?) in the Kenya 2017 Presidential Election."

[9] Kalinin, Kirill and Walter R. Mebane, Jr. 2016. "Worst Election Ever in Russia?"

[10] Mebane, Jr., Walter R., Patrick Wu, Logan Woods, Joseph Klaver, Alejandro Pineda and Blake Miller. 2018. "Observing Election Incidents in the United States via Twitter: Does Who Observes Matter?"

or wait-times of various lengths, success or difficulties voting, success or difficulties registering, participation in election-day, early or absentee voting, and more. At the time of the presentation, these incidents had been identified at more than 12,000 distinct locations in the continental United States (plus many locations abroad).

Using a measure of "presidential campaign partisan association" constructed using word embeddings derived from Twitter users' self-descriptions, we observe "communication silos" in which users tend to report their incidents to other users who have similar partisan associations. Users with differing partisan associations tend to report different kinds of incident—compared to "***clinton / hilary / hillaryclinton / strongertogether / democrat***" users, "***trump / donald / realdonaldtrump / maga / republican***" users are:

1. less likely to report unspecified line length incidents or long lines,
2. less likely to report unspecified polling place incidents, neutral polling place incidents or success voting,
3. less likely to report unspecified registration incidents or neutral registration incidents but more likely to report registration problems, and
4. less likely to report unspecified electoral system incidents or neutral electoral system incidents.

The reporting differences seem to reflect biases more than differences in real experiences. To implement the second version of the Observatory, we have used the Streaming API to collect about 65 million keyword-filtered original Tweets during October 1–November 6, 2018.

NEW STATISTICAL TECHNIQUES IN INTERNATIONAL PERSPECTIVE

EMILY BEAULIEU BACCHUS
University of Kentucky

Advances in the statistical techniques available for use in elections audits present exciting opportunities for those seeking to promote election integrity and strengthen the democratic process. At the same time, international experiences with elections provide several important points of consideration for election administrators, observers, and other actors providing technical assistance and support, even in the context of U.S. elections.

This presentation stressed the emphasis on a holistic definition of an election audit. Extending from this definitional orientation, the presentation emphasized: best practices for conducting audits, the critical importance of data availability, and the need for an appreciation of, and sensitivity to, the broader political context in which the audit takes place.

For international democracy promoters, an election audit is more than a recount.

While a recount can be employed to confirm results, an audit is a broader investigation (which may involve a recount) initiated in response to accusations of fraud, in order to verify the integrity of the election and establish whether election results should be considered legitimate. Thus, while both a recount and audit aim to determine whether election results are "correct," the charge of an audit extends beyond a narrow recount of ballots, to take a fuller picture of actions undertaken by key stakeholders and to evaluate the impact of those actions on election outcomes.

In the interest of accomplishing a more holistic audit, that assesses election integrity

rather than simply election outcomes, international practitioners have several ideas about best practices—all of which emphasize the need for election administrators to plan in advance for the possibility of an election audit.

First, any audit should ideally be undertaken by the country's own election management board (EMB). The emphasis on domestic election administrators performing an audit serves two purposes:

1. it prevents key stakeholders in the election (parties and candidates) from manipulating the election process (or being perceived as doing so).
2. It limits perceptions among stakeholders and the electorate of outside interference in the election process.

The main caveat to this advice is the recognition that some of the advanced statistical techniques being employed in election audits today may require expertise from third parties outside the country—such possibilities, however, should be planned for and made transparent well in advance of an actual audit.

Given that an election audit will include activities beyond a vote recount, the procedures and standards for the audit must be established well in advance. Audits that occur without such understandings in place are likely to do little to improve confidence in elections, or produce compelling evidence of election fraud.

In order to be legitimate, audit procedures should be constructed from a country's election law. These procedures must anticipate the kinds of issues that are likely to arise and trigger an audit, and make explicit plans to evaluate the election on the basis of those issues.

Finally, all the processes associated with the audit must be transparent and clearly communicated to key stakeholders (who should be able to observe, but not conduct, the audit). In particular, any advanced statistical methods that are employed in the course of the audit should be clearly communicated to stakeholders. Otherwise such evidence may undermine the credibility of the audit, which ultimately undermines the goal of evaluating the integrity of the election.

EXAMPLES:

» ***Venezuela Presidential Recall Audit (2004):*** The Carter Center worked with Venezuela's election commission, used simple statistical analyses, and addressed subsequent criticisms of the audit. This audit upheld the results of the election as valid.

» ***Haiti First-Round Presidential Audit (2010):*** The Organization for American States examined vote counts from outliers (high turnout, high vote margin) in a random sample of polling stations, in response to fraud accusations. Determined that 2nd and 3rd place in the first round should be reversed, affecting competition for the presidency.

While international democracy promoters stress these best practices for conducting an election audit, it is critical to acknowledge that a holistic audit requires data to be successful. The data made available to auditors should be extensive and include: voter registers, voter turnout, and election results data. Further, the turnout and results data should be disaggregated, ideally to the level of individual polling places. Finally,

data on the time that counts are taken, reported, and incorporated into higher levels of aggregation should also be collected and made available to auditors. If the country is using an electronic voting system, the codes used to transmit and aggregate results must also be made available to auditors.

This level of data availability requires first, that election management bodies establish procedures to collect the data and second, that election law permits such data to be made available to auditors in the event of an audit. In many countries today (e.g. Nigeria, Guyana, Cambodia) release of disaggregated results is not permitted once results have been aggregated and submitted to the central election management body. Further, issues and suspicions can be exacerbated when countries use electronic methods (or a mix of paper and electronic, as in Kenya) to aggregate election results. Finally, temporal data is critically important because demographic patterns can confound the meaning of irregularities that appear to be geographically distributed.

EXAMPLES:

- ***Kenya (2017):*** This election is an example of the limited conclusions that can be drawn when data are insufficient. Election results were aggregated both electronically and via paper ballot, but only electronic results were available for analysis. Furthermore, this is a country where demographic patterns make it difficult to draw conclusions from geographic irregularities, and time-stamped data would be useful.
- ***Honduras (2017):*** Because data was available at the polling location level, and by time of report and aggregation, this is a case where the Organization of American States was able to identify clear anomalies suggesting that there had, in fact, been fraud committed.

Photo credit: Annie Bolin

Finally, when undertaking an election audit, auditors and those overseeing the process must remain cognizant of the broader political context in which the election takes place. Again, if one thinks of an audit as analogous to a recount, in that it seeks simply to provide an accurate picture of what happened in the election, then the broader political context does not seem relevant.

Returning to the international definition of an audit, however, we know that these undertakings are motivated by accusations of fraud and electoral malfeasance. The kinds of elections where such accusations arise, are very often elections in political systems that are fraught with instability and the potential for conflict and/or democratic backsliding.

In such cases, those conducting the audit must way the value of providing accurate results against the value of maintaining peace and stability.

EXAMPLES:

- ***Afghanistan (2014):*** After accusations of fraud the United Nations supported an audit that included a full recount of all polling locations. The results of this audit, however, were never released publicly or to key stakeholders. Instead, the audit motivated a compromise between the winning and losing candidate for power sharing. This is an example where stability in the political systems was valued over electoral accuracy.
- ***Kosovo (2010):*** In this election an automatic, remedial audit was implemented where all tabulation sheets were checked against officially recorded results to ensure accuracy. Results of this audit were released publicly, showing that results from almost 50% of polling stations were inaccurate and should be invalidated. As a result, voter confidence in elections declined sharply, suggesting a case where accuracy was prioritized over enhancing confidence in democratic elections.

In sum, the international election perspective cautions us that election audits must be holistic, and well-planned in advance, and that data must be fine-grained, prolific, and made available to auditors. Finally, auditors are advised to consider the broader political contexts and must be alert to the potential for goals such as accuracy to be in tension with other goals such as political stability and the promotion of voter confidence in elections and support for democracy.

WHAT COLORADO CAN TEACH US ABOUT POST-ELECTION AUDITS

RISK-LIMITING AUDITS: LESSONS LEARNED

NEAL MCBURNETT
Independent Consultant

In 2017, Colorado became the first state to regularly conduct risk-limiting audits (RLAs). Colorado's successes are grounded in 15 years of multi-partisan efforts to promote and pilot election auditing. Here are some of the lessons I've learned along the way.

For more background, and links to a wealth of material, I encourage you to explore The Colorado Risk-Limiting Audit Project (CORLA), available online.

> ***One of the clearest lessons is that pilot audits with input from people experienced with risk-limiting audits are enormously helpful and highly recommended. The whole community learns from pilot audits.***

BEST PRACTICE: BALLOT-LEVEL RLAS

Colorado has demonstrated that with good systems, processes and data, you can do ballot-level risk-limiting audits which limit the risk that tabulation errors or attacks result in getting the wrong outcome. This can be done at scale, in hundreds of contests, in dozens of counties, and across overlapping districts in a state.

They can also be done efficiently. Colorado audited less than ten thousand ballots statewide. Besides the fully risk-limiting audits, simultaneous "opportunistic" audtis can gather evidence on and report risk levels for all the rest of the contests.

Furthermore, Colorado's new statewide system is among the most cost effective and best for auditing: central-count scanners with BMDs available for accessibility.

RESOURCES AVAILABLE

These highly efficient ballot-level RLAs can be done with equipment from multiple vendors. In 2015, four vendors presented and piloted systems that could do ballot-level comparison RLAs in 2015. They were all central count scanning systems, from Dominion, Hart, ClearBallot and ES&S

Colorado funded the development of software to help manage the audits, which is now the open source ***ColoradoRLA***. This system continues to be enhanced, and can be used for free by any jurisdiction, with support available from multiple organizations.

IMPORTANCE OF RLAS

> *There is widespread, transpartisan consensus on the need for both paper ballots and audits.*

An early example was in 2003, when four local parties (Republican, Democrat, Libertarian and Green) supported a joint consensus in Boulder, Colorado. An excellent overview of the modern case is in the National Academies report from 2018: ***Securing the Vote: Protecting American Democracy***, from The National Academies Press.

While we've made huge steps forward, there is still much to do. Why is it taking so long to adopt robust audits?

- Elections are increasingly complicated
- You can't easily audit the data you've got
- You can't easily get the data you need

This underscores why it is critical to support and adopt the Common Data Standards work by the EAC / NIST VVSG-Interoperability task force.

COMMON DATA FORMATS

We need format standards! See a helpful overview presentation by John Wack: ***Overview of VVSG-Interoperability Common Data Formats*** (two presentations).

Common data formats are published or in-the-works for several use cases. Election Results reporting (SP 1500-100) is used in OH, NC, LA County. Other states are in progress. The Election Log Export CDF will soon be published as SP 1500-101. The Voter Records Interchange CDF is slated for review by VR vendors, to be published as SP 1500-102. I have seen initial use in OH and by OSET.

The Cast Vote Records CDF schema should be published soon as SP 1500-103. The ongoing development and documentation of election process business models and voting method descriptions is also very beneficial.

EVIDENCE PRESENTED AND CHECKED

Audits which are conducted by elections officials should also be highly accessible to the public, and the critical inputs to and results of the audit should be shared openly. Otherwise, audits may be convincing to officials, but leave losing candidates and the public without enough evidence to go on.

A document presenting details on what the public should have access to is available at ***Public RLA Oversight Protocol***, by Stephanie Singer and Neal McBurnett, 2017. Briefly, the elements it covers are: Chain of Custody, Tabulation, Manifest, Commitment, Random Selection, Ballot Card Retrieval, Ballot Interpretation and Data Entry, Ending the Random Selection and Examination of Ballot Cards, Hand Count, and Audit Conclusions Affect Outcomes.

COLORADO AUDIT RESULTS

The ColoradoRLA software includes an `rla_export` tool to provide necessary data for Oversight Protocol in csv/json formats.

`rla_report` software is in progress to interpret the exported data, confirm that the right ballots were selected, and check the risk level calculations, to help implement these oversight steps. This code will also be open source, and verifiers should be encouraged to check it and/or implement their own oversight processes and code.

In its recent audits, Colorado has shared more useful data on its audits, in more useful ways, than probably any other jurisdiction. Officials can be very proud of their results. Officials with access to all the audit data, including the Cast Vote Records (CVRs) etc., can be more confident in the outcomes of more contests than anywhere else in the country, and certainly more efficiently than anywhere else.

CONVINCING OTHERS OF ELECTION OUTCOMES

Unfortunately, while this is much more transparency than in the past, losing candidates and the public still encounter several crucial holes in the oversight protocol. Some summary data is not available yet, principally because due to an unusual confluence of challenging circumstances, the state is still wrestling with ballot anonymity issues which have limited the availability of the original CVRs to the public. That means the public can't check tally totals, and can't check ballot interpretations in real time, or sometimes at all.

We give kudos to the amazing ongoing accomplishments by both the state and the counties under very challenging circumstances, and look forward to resolving the various obstacles to full transparency.

A model for that sort of transparency has already been seen in the audits in Boulder CO in 2008, which, before the audit, successfully generated auditable data. In some cases that required merging small sets of ballots into larger sets, all to be audited together, in order to eliminate anonymity concerns. See Boulder County 2008 General Election Audit for the data and open-source software for those batch-comparison audits.

More detail on relevant challenges and good solutions is available at ***Preserving Anonymity of Cast Vote Records***, by Mark Lindeman, John McCarthy, Neal McBurnett, Harvie Branscomb, Ron Rivest, and Philip Stark, 2017-08-03.

DISCREPANCY INVESTIGATIONS

Detailed reporting on discrepancies in Colorado's audits is still in-progress. But it is evident that there are still some instances of errors in data entry. To avoid that, the software should inform the Audit Board that there was some sort of discrepancy right after it has been officially entered (and after preserving a record of that official entry). That would help with discrepancy investigations, provide much more useful and actionable quality control feedback, and enhance trust in the process on all sides.

REMAINING CHALLENGES

The software needs enhancements in reporting convenience and analysis. It should make it easy to view discrepancies, and risk levels for opportunistically audited contests. That is particularly challenging for the wide variety of districts, each involving samples taken in a variety of counties. The software should also automatically generate an "Audit Center" web site with full data for the public.

The software should be further modularized for use with external risk-level calculation modules, covering additional auditing methods like SUITE, Bayesian RLAs, etc.

We need new approaches to handle in-precinct/vote center scanners, which randomize ballots and/or CVRs. They complicate the process of matching paper ballots with CVRs.

We need upgraded support for batch-comparison audits, which yield risk reduction which is predictable, easy to plan for and easy to understand. We should also provide better support for ballot-polling audits, though they can be unpredictable and impractical for some of the most interesting contests with tight margins.

We should foster collaboration between clerks, privacy experts, and tool-smiths around preserving anonymity, especially for the complicated situation in Colorado. And we should audit more systems involved in elections: voter registration, signature verification, envelope sorting, ballot reconciliation etc.

TARGETED AUDITS

Often in any given election, public attention is focused on particular circumstances. Random selection of ballots to audit is essential for good risk reduction, but we should also be prepared to directly address specific concerns and unusual circumstances.

We should encourage candidates and the public to identify additional interesting ballots to target for auditing. They could be chosen based on analysis of the CVRs, based on mark density data, or even based on ballot images.

PUBLIC ENGAGEMENT IN VERIFICATION

Finally, we should promote more public participation in audits. We could print ballot tracking pages with QR codes, and provide an app that public observers could use to photograph ballots along with the tracking-sheet QR codes. That could assist the public in conducting their oversight, and facilitate sharing of a series of confidence-inducing tweets like ***"I verified the votes on this ballot."***

ACKNOWLEDGEMENTS

I'm deeply grateful to Paul Tiger for being the first to encourage me to get involved in election verification back in 2002. A long list of colleagues since then have offered expertise, insights, enthusiasm, and comradery, including Joe Pezzillo, Paul Walmsley, Ron Rivest, Philip Stark, Harvie Branscomb, and Hillary Hall and her Boulder County team, The Election Verification Network has been invaluable in all of this work.

The Colorado legislators who helped us pass laws in 2005 and 2009 to require audits deserve much credit. I've been incredibly impressed at the dedication of the Colorado SOS staff and Clerks! The Free & Fair Team that took on the daunting challenge of signing up to write the initial ColoradoRLA software under incredible constraints of time and resources deserve my eternal gratitude. They went beyond the call of duty.

And the Democracy Works team that has continued to improve the software, enhancing the user interface and digging deep into the internals to re-work it for multi-county contests has been incredible also.

Updated versions of this narrative report will be available at http://bcn.boulder.co.us/~neal/elections/audit-summit.html

SUMMARY OF RLA IMPLEMENTATION: TRAINING AND CHANGE MANAGEMENT

HILARY RUDY
Office of the Colorado Secretary of State

RELATIONSHIPS AND COMMUNICATION

In our experience, one of the strongest factors to successfully deploying any major project or new system is building and maintaining strong working relationships between the state and counties, and with any outside vendors. The state leverages these relationships to gain buy-in and build support for the project, and to identify "cheerleaders" who will help test and pilot.

> *We've found that good communication is central to building trust and a strong relationship.*

A critical factor of success in project implementation is that counties must be comfortable calling with questions or training needs. It takes time and work to build trust, and face-to-face interactions are essential in the process. Our office goes out regionally to provide training and we attend the clerks' association conference. We also go out to visit the counties in their offices to understand their unique processes and specific challenges. Having established relationships helps our team plan resources and focus their energy on counties that may need more one-on-one training time.

We've found that it's critical for our team to be responsive when the counties call in with questions or need one-on-one training time. The team reaches out regularly to the counties to ensure they feel a level of comfort calling in. We layer the communication to counties and focus on ensuring that our messages are clear and effective. The voting systems manager sends regular emails to the counties listing upcoming deadlines and critical information. We include the same information in the weekly newsletter that we send to counties. And leading up to

the mock risk-limiting audit before the 2018 general election, we also highlighted in the weekly newsletter one piece of functionality in the audit system that had changed. We conduct a weekly county support call during the election period, and we include the upcoming deadlines and other critical information in that weekly agenda.

Before the first statewide audit, the team developed clear, comprehensive written documentation about the process and technology. This documentation also included how to use the ancillary systems, such as how to hash a document or access the SFTP site. In addition to the state's step-by-step technical documentation, we worked with the counties to develop a county playbook outlining process best practices for small and medium counties. We work with the counties to update the documentation before each audit to ensure it's accurate, comprehensive, and understandable.

Trust and communication are critical to implementing large statewide projects—we can continue implementing big changes when there are simultaneous implementations that place a strain on the counties' resources. For example, in the 2018 general election, we implemented a significant change to how the statewide contest is audited. It worked and the audit ran smoothly because counties called with questions and the team spent a lot of time working one-on-one with them.

LAYERED TRAINING

Another factor of our success is approaching training as an iterative process. It's essential to establish and maintain a safe learning environment where everyone feels comfortable asking questions openly and honestly. If counties are honest about their challenges, the resulting discussion is more productive in terms of identifying real workable solutions.

We begin with general concepts and terms to help counties understand the legal and philosophical framework. Then we cover why the process or project is being implemented and any way in which the counties will benefit from the change. Helping counties understand 'why" is fundamental to gaining buy-in. It's also important to train on legislation or rules that are changing as well as the legislative and rule process, and to recognize that legislative and rule changes may need to be tackled iteratively to avoid unintended consequences.

We've found that it's important to cover the technical steps of the process, in this case the audit, at several points during the training cycle. But it's most critical during the process discussions and the hands-on training. As I discussed in the communications section, comprehensive guides for both software and processes are important. Guides should be step-by-step manuals that include screenshots and explanations of ancillary systems like the hashing tool. And they should be updated regularly to reflect technology updates and feedback from the counties.

Training around process improvement and change management in general is also a key factor of successful project implementation. In other words, how do we evaluate our processes, document them, and identify opportunities for efficiency. We also always try to bear in mind that one-size fits all processes generally aren't the most effective. What works for a large county with urban populations isn't going to translate well to a small rural county for several reasons, including resources, budget, and technology.

One approach we've found to be incredibly effective is to train to the goal and then crowdsource the solution. Get counties with similar populations, budgets, resources, and challenges together and work collaboratively to develop the business processes. This approach ensures that we develop good processes and it helps gain buy-in because it's not just a process mandated by the state.

When identifying process changes, we've also found that it's important to minimize significant disruptive changes, which can create confusion for pollworkers. Rather than implementing wholesale and overwhelming changes, which increase the risk of failure, we look for ways to streamline existing processes for efficiency and incorporate small adjustments. And with all changes, practice makes better. It's beneficial to practice and test the new processes to make sure things will work as expected. In addition to the counties conducting process walk-throughs, we also place a focus on hands-on training in the software.

Hands-on practice and mocks are one of our most effective training tools. We try to allow as much practice in the system as possible to build muscle memory. Colorado conducts a mock risk-limiting audit before every election. It gives the county staff and audit judges an opportunity to learn in a safe, but realistic, environment.

We believe it's important to treat a mock as a training exercise and respect the safe learning environment. We work to make sure it's safe to fail and learn from it. During the mock, the voting systems team spends a lot of time one-on-one with counties making sure they're comfortable and all of their questions are answered. They also work with counties to walk through any errors in the mock to explain how it would affect that county and the entire state in a real audit.

DEBRIEF AND IMPROVE

Following each audit, we solicit and listen to county feedback about the processes and the system. This has led to system enhancements for usability to help reduce errors as well as changes to the training and documentation. The team updates the instructions and documentation based on the feedback and resulting system changes, and we work with the county clerk's association to update the county process playbook.

It's also critical to continue providing refresher training. We survey following every training to ensure the training is meeting the counties' needs. And we've consistently found that the survey responses support a need for continual training. Finally, as we implement we try to keep the end goal in mind; what are we working to accomplish and why, and how can we work with our county partners and other stakeholders to ensure success.

LOOKING BEYOND COLORADO: CHANGING TECHNOLOGY AND STATE POLICY

LOOKING BEYOND COLORADO: RISK LIMITING AUDITS IN INDIANA

JAY BAGGA
BRYAN BYERS
Indiana Voting System Technical Oversight Program (VSTOP)
Ball State University

INTRODUCTION

The Indiana Voting System Technical Oversight Program (VSTOP) has recently been involved in risk-limiting audits and other election activities related to physical and cybersecurity of election systems in Indiana. This report presents a brief description of such activities.

VSTOP was established by Indiana statute in 2005 (P.L.221-2005, SEC.95). In 2008, the Indiana Secretary of State contracted with Ball State University to manage the operations of VSTOP. Since then, VSTOP has worked with the Indiana Secretary of State and the Indiana Election Division to manage many election-related activities, including developing and proposing procedures and standards for the certification, testing, acquisition, functioning, training, security for voting systems and electronic poll books used to conduct elections in Indiana, establishing and managing an inventory database of election equipment in the 92 counties in Indiana and offering a Certificate Program in Election Administration, Security and Technology (CEATS) to county election officials within the state.

LANDSCAPE OF ELECTION SYSTEMS IN INDIANA

The 92 counties in Indiana are served by five voting system vendors and five electronic poll book vendors. About half of the counties use DREs. The other half use OPSCANS or a combination with DREs.

To be certified for use in elections in Indiana, a voting system must comply with, among other requirements, the 2002 Voting System Standards (VSS), or the 2005 or 2015 Voluntary Voting System Guidelines (VVSG). VSTOP developed a protocol for certification of electronic poll books in In-

diana. According to the National Conference of State Legislatures, Indiana's 2013 e-poll book legislation is currently the most comprehensive in the country. Since 2013, the number of counties in Indiana using electronic poll books has grown rapidly (currently at about two-thirds).

INTEGRITY OF ELECTIONS AND SECURITY OF ELECTION SYSTEMS

Each year, the Bowen Center for Public Affairs at Ball State University conducts the annual Hoosier Survey, which aims to gather public opinion data on current issues and provides that data to policymakers. The 2017 survey included the following question:

> *What level of confidence do you have that your vote in the last election was properly recorded and accurately counted?*

The table below includes the responses of a random sample of 600 Indiana residents, showing that about 40% of the respondents are not very confident.

These findings indicate a lack of confidence among a sizable proportion of Indiana residents. Public perceptions are important indicators of areas where public officials may need to address concerns. A number of initiatives have been undertaken by the Indiana Secretary State and the State of Indiana to address issues with security and integrity around Indiana's elections. Elections are included in one important initiative within the state launched in 2017.

The Governor of Indiana established the Indiana Executive Council on Cybersecurity (IECC) in 2017 to *"... form an understanding of Indiana's cyber risk profile, identify priorities, establish a strategic framework of Indiana's cybersecurity initiatives, and leverage the body of talent to stay on the forefront of the cyber risk environment."* The IECC comprises several committees including the Elections committee, chaired by the Secretary of State.

Members of this committee include, as representatives, County Clerks, the Indiana Election Division, the Indiana Office of Technology, the Statewide Voter Reg-

CONFIDENCE LEVEL	PERCENTAGE
VERY CONFIDENT	60%
SOMEWHAT CONFIDENT	23%
NOT TOO CONFIDENT	8%
NOT CONFIDENT AT ALL	9%
DON'T KNOW/REFUSED TO ANSWER	<1%

istration Commission, and VSTOP. The committee has made several contributions including a review of the physical and cybersecurity aspects of elections, voting systems and electronic poll books, recommendation of best practices, and risk-limiting audits.

RECENT AND PROPOSED LEGISLATION

The 2018 Indiana Senate Enrolled Act (SEA 327) brought several physical and cybersecurity policies into law, including secure custody, sealing and storage, and inventory and disposal of election equipment. Under current law (IC 3-12-3.5-8), Indiana has some post-election audit requirements. Proposed legislation in the 2019 Senate Bill SB 570 includes voter verifiable paper audit trail (VVPAT) requirements and risk-limiting audits in the coming years.

SB 570 also includes national criminal history background checks of vendor employees, a requirement that polling places comply with the Election Infrastructure Outreach Security Checklist published by the United States Department of Homeland Security and a requirement that all problems or anomalies with the functioning of voting systems and electronic poll books be reported to the Secretary of State within 48 hours of its discovery.

RISK-LIMITING AUDITS

As part of its work with the IECC, VSTOP conducted the first ever RLA Pilot in Indiana in May of 2018. Dr. Ronald Rivest of MIT and Mr. Jerome Lovato of EAC assisted in this effort, among others. The RLA was conducted in Marion County, Indiana which includes the city of Indianapolis. Several weeks were spent in the preparation of this RLA. The RLA concept was totally new to Marion County and there was some initial reluctance. However, after discussion and several presentations, the county became quite interested in being part of the pilot. Substantial help was provided by the Marion County Clerk, Director of Elections, Deputy Director of Elections and their staff. The project was fully supported by the Indiana Secretary of State Connie Lawson.

In the Marion County RLA, three races were audited, the 2016 Presidential Election (5 precincts, Ballot Polling), the 2018 Primary Democratic Sheriff (10 Precincts, Ballot Polling) and the 2018 Republican U.S. Senator (10 Precincts, Comparison Polling). Both the Stark Method Risk Limit (10%) and the Bayesian Method (Bayesian Limit 5%) were employed. The first RLA confirmed Clinton as the winner in the precincts audited for the 2016 general election for President.

This was a fully completed RLA. The other two audits were ceased early due to time constraints. It is noteworthy that this was the first time that the Bayesian Audit Method was used in the field.

Jay Bagga and Bryan Byers presented the results of the Marion county RLA at the 8th annual national conference of the State Certification Testing of Voting Systems held in Raleigh, NC in June 2018. VSTOP also assisted with the organization of the RLA Pilot in Michigan that was led by Liz Howard of the Brennan Center.

The positive experience gained from the Marion county audit led the Secretary to ask VSTOP to conduct a second county wide audit of several races in Porter County, Indiana. This audit was conducted in January 2019 and included five countywide races (123 precincts): Public Question #1, Coun-

ty Prosecutor, County Auditor, County Recorder and County Coroner. The Porter County RLA was one of the most comprehensive local RLAs conducted in the United States and VSTOP was able to acquire valuable information about pre-election preparation, poll worker training, ballot chain-of-custody, post-election processes, and time and budget efforts for RLAs. The Three-Cut ballot sampling method facilitated efficient sampling and tabulation. Even with the ease of use and quick ballot polling, more time was still needed to sample additional ballots for the Recorder and Coroner races due to a substantial number of undervotes.

SUMMARY

The Voting System Technical Oversight Program (VSTOP) has been in existence since 2008. VSTOP's activities are wide and varied but are all concerned, in one way or another, with the integrity of elections and the security of election equipment. VSTOP has conducted two RLAs: Marion County (May 2018) and Porter County (January 2019. Both of these RLAs were successful, with the Porter County RLA being one of the most comprehensive ever performed.

The State of Indiana has taken many initiatives (including legislation) to secure elections and subsequently enhance voter confidence in election processes and outcomes. Should legislation regarding VVPATs and RLAs pass, VSTOP will be directly involved in the certification of VVPAT equipment and the implementation of Risk-Limiting Audits.

VOTING TECHNOLOGY & POST-ELECTION AUDITS

JEROME LOVATO
U.S. Election Assistance Commission

SUMMARY

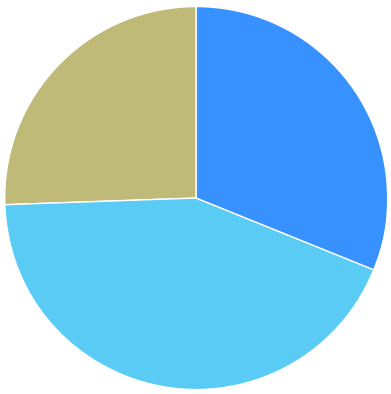
The decentralization of U.S. elections makes election administration very complex. One element of this complexity is voting technology and the ability to conduct risk-limiting audits (RLA). In this paper I will highlight three limitations of conducting RLAs, three ways to improve current voting system design,[1] and project what the future of RLAs look like with the advancement of voting technology and standards.

[1] *Voting system* refers to the total combination of mechanical, electromechanical or electronic equipment (including software, firmware, and documentation required to program, control, and support the equipment) that is used to define ballots; cast and count votes; report or display election results; and maintain and produce any audit trail information; and the practices and documentation used to identify system components and versions of such components; test the system during its development and maintenance; maintain records of system errors and defects; determine specific changes to be made to a system after the initial qualification of the system; and make available any materials to the voter.

WHERE WE ARE

The U.S. Election Assistance Commission (EAC) is responsible for developing and maintaining the Voluntary Voting System

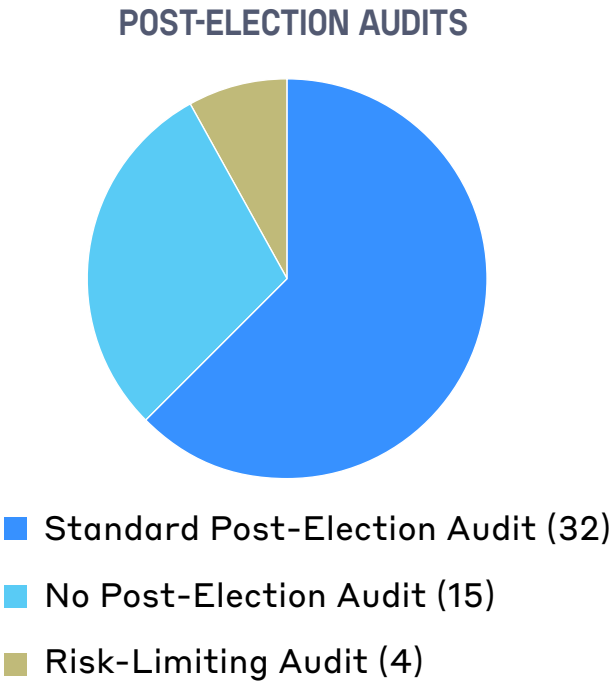
TESTING TO FEDERAL STANDARDS



- Full Federal Certification (16)
- Testing to Federal Standards (22)
- No Federal Requirements (13)

Guidelines (VVSG). The VVSG are specifications and requirements by which voting systems are designed and tested. These specifications and requirements are voluntary, which means that states are not required to adopt these standards to test and certify their voting systems. At a minimum, most states (including Washing D.C.) require testing to federal standards (see graph on the previous page).

Along with the diverse voting system requirements are even more diverse post-election audit laws. Due to this diversity, I have placed post-election audits in two categories: Standard and RLA. The figure to the right here shows the number of states (including Washington D.C.) that conduct standard post-election audits, the number of states that do not require a post-election audit at all, and the number of states that require an RLA.



CURRENT LIMITATIONS

I have identified three limitations for conducting RLAs: a lack of paper ballot records, data exports from voting systems, and state-level certification requirements. This is not an all-encompassing list of limitations, but is a high-level "top 3" list.

The lack of a paper ballot record is the most obvious limitation for conducting RLAs. The simple solution is to just require that all voting systems produce a voter verifiable paper ballot record. However, this "simple" solution isn't so simple when election officials must consider other factors such as: legislation, budget, and training. How much will a new or modified voting system cost? How much will voting system certification cost and how long will it take to be certified? How much will it cost, and how long will it take, to implement a new voting system? What changes to election law will be needed to address RLAs? What resources are available to train local election officials on how to conduct RLAs, and how long will that take?

Voting systems produce a vast amount of data along with options to export that data. An essential export for conducting a ballot comparison RLA is a ***cast vote record***.[2] The export file formats vary for each voting system. For instance, some systems produce exports in JSON, others in XML, and others in CSV. Although these are commonly used data formats, the confusion arises in interpreting these files (i.e. what data is relevant for conducting the audit). Some formats are not human readable. For the files that are human readable, additional massaging of these files are required to make them intelligible.

[2] Permanent record of all votes produced by a single voter whether in electronic, paper or other form. Also referred to as ballot image when used to refer to electronic ballots.

A not-so-obvious limitation for conducting RLAs is varying state-level certification requirements. For example, consider the following scenario:

> *Voting System, Inc. develops Voting System Model Y2K and sells it to multiple states. Two states: State A and State Z, like the Model Y2K, but they have specific requirements that must be met. State A requires state-specific reports; State Z requires state-specific functionality. Voting System, Inc. decides to sell Model Y2K.1 to State A to produce the necessary reports, and Model Y2K.2 to State Z to address the necessary functionality.*
>
> *After the purchase, legislators in both states pass laws that require ballot comparison RLAs. Now, both states need additional exports that are only available in Model Y2K.7. Voting System, Inc. offers to upgrade State A to Model Y2K.7.1 and State B to Model Y2K.7.2, but it will require additional funds since a free upgrade was not included in the original contract.*

And that is a snippet of the complications that exist with varying state-level certification requirements.

CURRENT DESIGN

Three areas where voting system design can improve to assist with conducting RLAs are human-readable cast vote records, ballot imprinting, and independent verification.

Voting system manufacturers should work to produce human-readable cast vote records. Election officials and auditors should not have to use third-party utilities or devote additional resources to read cast vote records. It is recommended that the cast vote record be in a tabular format where each row of the table represents one paper ballot record.

Imprinting a unique ID on a ballot improves the efficiency of conducting a ballot comparison RLA. The unique ID should not be imprinted on sections on the ballot that will cause the ballot to be unreadable by the ballot scanner. The unique ID must not be able to tie a ballot back to the voter. Finally, the unique ID should be a field in the cast vote record. For example, if the unique ID on the ballot is "A-1111" then the cast vote record should reflect "A-1111" not "1111."

A basic principle of RLAs is that they provide independent verification of the results of an election. With that in mind, a voting system should not be designed to include an "RLA module" or any other self-auditing utility. Paper ballot records and proper ballot management and security are all that is needed to conduct an RLA.

FUTURE TECHNOLOGY

What lies ahead for the future of voting technology? Within the upcoming year, the EAC will publish ***Voluntary Voting System Gudelines 2.0***, which will include interoperability requirements. Part of the interoperability work includes creating common data format (CDF) standards for cast vote records, election results reporting, election event logging, and voter records interchange. CDF standards will make RLAs and other election-related audits much easier since it will eliminate the head scratching that exists today of wondering, "What am I even looking at?"

Other technology that is in the early stage of development is voting systems that use blockchain (i.e. UOCAVA ballot delivery) and end-to-end verifiable voting systems.

SOFTWARE SUPPORT FOR RISK-LIMITING AUDITS

MARK LINDEMAN
Verified Voting

Why do we need software to support risk-limiting audits? Many people I talk with assume it is because we need to do complex statistical calculations—because they've been told that risk-limiting audits are a statistical method. That's fundamentally mistaken, in much the same way it's mistaken to think of a meeting room as an engineering model. In audits, as in architecture, it's important to get the math right so nothing collapses, but the math itself is not the point.

Risk-limiting audits are a kind of tabulation audit, which means that at their heart, they're about having people manually examine a sample of voted ballots to check the voting system counts. Most of the work is about helping people manage paper, and to record what they see on the paper. The math is not the territory.

In this context, there's sometimes a disconnect between how statisticians talk about risk-limiting audits, and how election officials and others do. Are risk-limiting audits hard, or are they easy? From a statistical standpoint, many risk-limiting audits are easy: the underlying principles are explicable, the methods are straightforward, and sometimes the calculations can be done with pencil and paper.

In the real world, risk-limiting audits can get hard in at least two senses. First, in many jurisdictions, managing all the voted ballots in ways that support efficient auditing poses multifaceted logistical challenges. Second, election processes have a dizzying array of variations—voting method or methods, equipment, ballot design and differences, the number of sheets per ballot, and the time available to conduct audits – that efficient audit designs must or should

accommodate. Sometimes these accommodations complicate the statistics; more often, they require new features or subtle variations upon existing ones.

> *Risk-limiting audits are easy in some ways, but they aren't ramen-noodle easy: they're complicated because elections are complicated.*

Good audit design requires close collaboration between election officials and various kinds of domain experts to address specific goals in specific circumstances. Naturally, that affects software development.

A brief first-person case study: The city of Fairfax, Virginia, conducted a risk-limiting audit pilot in August 2018, in cooperation with the Virginia Department of Elections and Verified Voting. The pilot included a ballot-level comparison audit based on a retabulation of all the ballots cast in the June Republican primary (under 1,000 ballots), as well as a ballot-polling audit. I wrote the support software. It provided support for rescanning the voted ballots in batches, automatically interpreting the votes, manually reviewing apparent overvotes, selecting a random sample of ballots, retrieving those ballots from various batches, and entering the audit team's interpretation of the votes.

I spent maybe a few hours writing code to compute the statistics. Mostly I worked with election officials to design the audit procedures – specifying in detail what people would do with the paper ballots at every step – and then customized the software to be as helpful as possible.

In Fairfax, I wrote most of the audit code from scratch in Python, incorporating an open-source sampling algorithm written by Ron Rivest and the OpenCV computer vision library. Why did I do that? There is quite a bit of prior art on risk-limiting audit software, and much of it is open source. Let me briefly enumerate some of it.

- Philip Stark has two web pages that can be used to conduct audits from beginning to end. That's not an abstract possibility: several counties have used these tools.
- Ron Rivest and collaborators at MIT have developed several codebases including the GitHub ***bptool*** and ***bctool*** repositories, which provide support for Rivest's Bayesian audits.
- Open-source R and Python libraries referenced in the election audit literature support many of the basic concepts, although there has been no systematic effort to build out these offerings.
- Free & Fair developed the original open-source software implementation for Colorado's statewide risk-limiting audit in 2017—often called the "RLA tool."
- Democracy Works developed the 2018 version of the Colorado RLA tool.
- And a group of pro bono developers are working to integrate and extend some of these tools to support risk-limiting audits in Rhode Island, starting with a January 2019 pilot.

So, with all this software available for reuse, what was I thinking? If you've developed software or used it in your research, you probably can imagine how things were for me. You want to solve a problem, Various people say, "Oh, no worries, there are some fabulous open-source tools that do what you want." So you start looking around, and you find a bunch of tools. You can't get some of them to run because of mysterious software dependencies. With others, the documenta-

tion is so crude that it's hard to tell exactly what they do, or how they could be adapted to your specific use case. Maybe one is great for a distributed application with dozens of clients (e.g., many counties conducting an audit simultaneously), but seems unwieldy for standalone use. Eventually you may find yourself writing software that has the functions you want, isn't cluttered with functions you don't need, and will be easier for you to customize because you understand its assumptions and limitations.

That's what I did. Unlike the Colorado RLA tool, the Fairfax software supported rescanning and automatically interpreting ballots, and the user interfaces were designed for readability when projected on a wall. Also unlike the RLA tool, it could only handle one ballot style and one plurality contest. It was exactly what we needed at the beginning of August, and what I could write in about six weeks while doing the rest of my day job at Verified Voting.

The June 2018 RLA pilot in Orange County, California took a different path. Neal McBurnett and Stephanie Singer, who collaborated on the technical support, reused and extended Free & Fair's version of the RLA tool. This required some interesting improvisations, because the RLA tool did not support ballot-polling audits – even though, conceptually, ballot-polling audits are simpler than the ballot-level comparison audits that the RLA tool does support! But this approach did prove workable.

So, on the software side, we have a growing number of codebases, many of which are written or customized for specific cases. That's partly because the development efforts tend to have small or nonexistent budgets, limiting the capacity to write code that can be readily extended beyond the problem at hand. The two iterations of the Colorado RLA tool are the most ambitious, but the state of Colorado could not, and did not, pay for an all-purpose customizable audit tool. We face a collective action problem: the governmental entities that could benefit from a large investment in open-source audit software for shared use have no means to pool their resources in order to obtain it. This problem seems eminently solvable, because the necessary seed investment is not very large: half a million dollars would go a long way. A collaborative project that engages software developers, election officials, other domain experts, and philanthropic support to support risk-limiting audits is well within our collective competence.

I have focused on how software development can address the problem of diverse needs—but we also have opportunities to simplify the problem itself. Currently, audit solutions must contend with a Babel of incompatible vendor data interfaces and election-office improvisations. NIST working group have been developing a series of Common Data Format (CDF) documents, including a forthcoming CDF specification for Cast Vote Records – the interpretations of individual ballots that are used in ballot-level comparison audits. Widespread adoption of CDFs and other interoperability standards will facilitate future audit implementations and other election innovations.

Working to implement statistically rigorous post-election audits sounds dreary; "a software developer, a statistician, and an election official walk into a bar" sounds like bad comedy. (It probably is.) But it turns out that we have a lot to say to each other, and we all enjoy solving problems together. Who knew that "limiting risk" could be so much fun?

NEW DIRECTIONS FOR COMPREHENSIVE AUDITING AND FORENSICS

A METHOD TO AUDIT THE ASSIGNMENT OF REGISTERED VOTERS TO DISTRICTS

BRIAN AMOS
University of North Florida

MICHAEL MCDONALD
University of Florida

Ensuring election officials give voters the correct ballot appears to be an easy task. However, three recent elections demonstrate consequential administrative errors happen:

In June 2018, dozens of voters in Habersham County, Georgia received a letter from their county's Office of Elections and Registration informing them that they had been assigned to the incorrect State House district. The 2018 Republican primary was decided by just 67 votes, the losing candidate challenged the results, and a judge ordered a re-vote.

In 2018, election officials discovered twenty-five homes along a stretch of road in Hamden, Connecticut were never assigned to their new district following the 2012 redistricting, leading to voters casting ballots in the wrong district across several elections.

In 2017, at least 384 registered voters in northeastern Virginia were assigned to incorrect State House of Delegates districts, of whom at least 147 cast a ballot. 125 of these were voters incorrectly assigned to House District 28, a number greater than the Republican candidate's 82-vote margin of victory.

From a naïve viewpoint, elections officials should easily determine which district voters' addresses are located in. In practice, election officials use data-driven representations of a jurisdiction's geography to manage the scale of assigning thousands of voters to the many overlapping districts and precincts in their jurisdiction. Intrigued by these situation, we developed a methodology to audit the assignment of registered voters to districts, and worked with Colorado and Florida election officials to identify three mechanisms that lead to district assignment errors:

Human error. This mundane error occurs when human operators make data entry errors into election management databases. These errors take different forms, depending on the management system. A frequent error involves databases of street address segments, which are street address ranges (e.g., 100 to 198 of the even side of Main Street) that are associated with districts. Election officials relate street address segments to voter registration database addresses, to assign districts to individual registered voters. A data entry error in a street segment database creates district assignment errors for an entire street segment, which is easily observed when affected residences are overlaid on satellite imagery maps. The district assignment errors in Hamden, Connecticut has the markers of such human error.

Geocoding error. Some election officials use geocoding processes to assign voters to districts. Geocoders have different levels of accuracy for the latitude and longitude coordinates they assign to an address. The most accurate level is what is known as "roof-top" accuracy, wherein a geocoding database provider has an accurate latitude and longitude point for a known address, often obtained from local government records. Geocoding programs use algorithms to guess at a latitude and longitude when they encounter an unknown address. For example, a geocoder may guess that 150 Main Street lies midway between the endpoints of the 100 to 198 even side of the Main Street segment. There are two necessary assumptions for such algorithms to work well: a street lies in a straight line, and the correct setback distance from the street to the building is used.

Geocoding processes are not panaceas. Geocoding databases and algorithms are often proprietary, created through different processes, such that they can produce different results. We identified and verified district assignment errors even when election officials use a geocoding process to assign voters to districts. Assignment errors that appear to be caused by non-linear streets and setback issues are more prominent in rural areas, but we have observed these issues in urban areas, too. In one case, we identified an assignment error for a large apartment complex with hundreds of registered voters.

Asynchronous data. Assignment errors may arise from a geocoding process that uses out of date data. Among the more esoteric errors we observed occurred in Colorado, where their geocoding process to assign registrants to districts used district boundaries based on 2013 Census Bureau geographic data, while their geocoder used updated 2017 data. Subtle changes in the 2013 to 2017 census geographical data resulted in district assignment errors.

Briefly, our audit methodology works in the following steps:

1. ***Obtain a voter registration file.*** These data contain two important pieces of information for our purposes: voters' addresses and the districts they are assigned to.
2. ***Geocode voters' addresses.*** We find using multiple geocoding databases provides greater successful geocoding of a voter registration database. A frequent issue we observe using a single geocoding database is street name changes, which may be updated in a geocoding database, but persist as legacy addresses in a voter registration database.
3. ***Obtain district boundary files.*** The Census Bureau disseminates boundary data for congressional and state legislative districts. Collecting data on other statewide districts and local district is deeply challenged.
4. ***Perform a spatial join.*** We overlay the point locations of geocoded voter registration addresses, and their associated district assignments per the voter registration file, on the district boundaries and note where the district identifiers are different.
5. ***Verify potential errors.*** We check each suspect address by overlaying the data we generate onto satellite imagery. This helps confirm that a building is indeed located at the latitude and longitude identified by the geocoding software.
6. ***Generate reports.*** We generate lists of suspect addresses, accompanied with maps of district boundaries and dots locating suspect addresses overlaid onto satellite imagery.

The good news is that we can audit district and precinct assignments. Technological innovations have progressed such that it is possible to develop and deploy auditing systems, and we recommend election officials to take advantage of them. Indeed, some vendors have deployed systems to report on the assignment of registered voters to districts, similar to the methodology we describe. However, even when election officials use such systems, we recommend an external audit since they depend on geocoding databases that may themselves have errors.

The result of these efforts will be better election data integrity, which will improve voters' experiences, reduce election costs, and improve voters' confidence in the electoral system.

PUBLICLY-VERIFIABLE ELECTIONS

JOSH BENALOH
Microsoft Research

Electoral systems in the United States are easy targets for attackers. As observed in the recent report from the National Academies of Science, Engineering, and Medicine, ***Securing the Vote: Protecting American Democracy***, our systems for casting and counting of votes are extremely vulnerable. The standards and practices in election systems do not compare with those of most industries, and they fall far short of the level that should be achieved by such a critical infrastructure.

However, it is important to recognize that while industry best practices should be applied, this isn't enough. Most of the over eight thousand election jurisdictions in the U.S. are small and lack a dedicated staff of information technology professionals. But many attacks come from nation-states with vastly superior resources and expertise. The battle is asymmetric, and it is simply not realistic to assume that it is possible to make our electoral system impervious to all possible attacks. We can, however, build a robust auditing infrastructure that allows us to know if any of our elections have been tampered with.

There are two basic varieties of audits:

1. Process audits allow administrators or third-parties to look at equipment and procedures to ensure that best practices are being applied.
2. Tally audits allow parties to verify the correct recording and counting of votes.

Within this second category, there are again two varieties:

1. Administrative audits allow election administrators to statistically sample ballots to confirm that they are consistent with the reported tallies.

2. Public audits allow independent observers and voters themselves to confirm that their ballots are correctly recorded and tallied.

While administrative audits, such as risk-limiting audits, are quite valuable and should be conducted for every contest in every election, they can be cumbersome and do little to provide confidence to a voter or observer who does not trust election administrators to properly maintain original ballots or to conduct their audits in ways that are fully independent of the original tallying.

In contrast, public audits allow skeptical parties to verify the accuracy of tallies themselves—without having to delegate trust to third-parties. The primary means for public auditing is a set of technologies that achieve what is known as ***end-to-end (E2E) verifiability***.

An election is said to be end-to-end verifiable if the following two properties hold:

1. *Voters can verify their own votes have been properly recorded.*

2. *Any observer can verify that all recorded votes have been correctly tallied.*

E2E-verification depends on the public, rather than election administrators, to perform auditing tasks. In high-profile elections, this may be commonplace. However, there is no guarantee that sufficient public attention will be paid to lower-profile elections. This is just one of several reasons for every election to also undergo administrative auditing.

It is easy to see how the requirements of E2E-verifiability can be achieved in open-ballot elections. Voters can convey their selections to election administrators who then post all votes—together with the names of the voters who cast them—in a public place such as a (digitally signed) web page. Voters can easily see that their votes are correctly recorded, and any observer can easily tally the votes to confirm that they correspond to the announced tallies. (A digital signature deters a malicious administrator from showing different posts to different viewers—since discovery of two distinct signed lists immediately implicates administrators as acting improperly.) The challenge is to achieve E2E-verifiablity in secret-ballot elections, and the typical mechanism is to post encrypted votes rather than open votes.

When posted votes are encrypted, achieving E2E-verifiability requires providing voters with means to confirm that the encrypted votes associated with them represent their actual selections (and this must be done in a way that does not allow voters to reveal their votes to others) and a mechanism must be provided to allow observers to verify that the encrypted votes accurately reflect the announced tallies.

There are multiple ways in which each of these tasks can be achieved. Numerous innovative mechanisms have been developed that allow voters to confirm the correct recording of their votes. Most don't require voters to take any extraordinary steps and do not impose additional burdens on voters who choose to avail themselves of this capability. The common element is that almost all of these systems provide voters with take-home receipts that can be used to track their votes. These receipts do not allow voters to see their actual selections nor

to show them to others. Instead, they allow voters to confirm that their votes have not been changed since the time that they were cast (when voters could confirm their actual selections).

The verification of tallying typically requires sophisticated cryptographic methods—often employing ***homomorphic encryption***. Homomorphic tallying allows encrypted votes to be directly amalgamated in encrypted form to construct an encrypted tally. This amalgamation can be repeated and checked by any observer and often is no more complicated than multiplying the encrypted ballots together. This aggregate encryption is then decrypted by election administrators who also provide a proof that allows observers to independently verify that the decryption is correct.

An alternative approach, known as a ***Mix-Net***, allows the encrypted ballots to be publicly shuffled while preserving their contents. Election administrators or others can serve as shufflers, and a proof must accompany each shuffle to demonstrate that the contents haven't been altered (the shuffling and proof typically use homomorphic encryption methods—although they do not employ homomorphic tallying). Once all of the encrypted ballots have been sufficiently shuffled, each ballot is individually decrypted by election administrators—who also provide independently verifiable proofs of each decryption. The open ballots (now dissociated from the voters who cast them) can be independently tallied by any observer to confirm that the announced tallies are correct.

With both homomorphic tallying and Mix-Nets, there is generally not a single decryption key. Instead, the key generation process is usually distributed so that multiple authorities must cooperate to form a decryption. Ideally, threshold encryption is used so that, for instance, three of five election authorities must cooperate to decrypt. This distributes the decryption capabilities so that a single rogue entity cannot compromise privacy while providing robustness so that a minority cannot prevent an election from completing.

The collection of technologies that enable public verifiability of election tallies provides a valuable complement to risk-limiting audits and similar administrative auditing methods. When used together, public and administrative audits can engender strong public confidence in the accuracy of election results.

DESIGNING BALLOTS FOR VOTERS AND ELECTION WORKERS—AND AUDITS

WHITNEY QUESENBERY
Center for Civic Design

At first, it wasn't entirely clear how ballot design fits into a conference on election audits. In all the discussions about the mathematics and 12-sided dice, it's easy to lose track of the goal: to ensure that the connection between voters and the results of an election is not broken. That is, an audit asks whether the ballots in an election were counted as they were cast, so perhaps we should also consider how to ensure that voters have the best possible opportunity to mark, verify, and cast a ballot that reflects their intent.

Phillip Stark famously said "an audit is no better than the paper trail it uses." I completely agree with that. Of course paper ballots are essential as a record of voter intent.

> *But, I disagree that a hand-marked, optical scan-style paper ballot is the only ballot design, or even a 'gold standard.'*

In fact, we have a long, rich history of ballot design that has fooled voters and has sometimes arguably affected the outcome of an election. Many of us are in this field today because of the butterfly ballot in Palm Beach County, Florida in 2000. But there have been many other examples before and since.

We know the problems and have strong research and empirical election evidence for best practices and the designs that cause problems: Contests that are split over two columns cause overvotes. Open primaries with two party elections on the same ballot invite people to vote in both, and throw away their vote. Confusing instructions, too small text, weak alignment between the marking target and the candidate. Sadly,

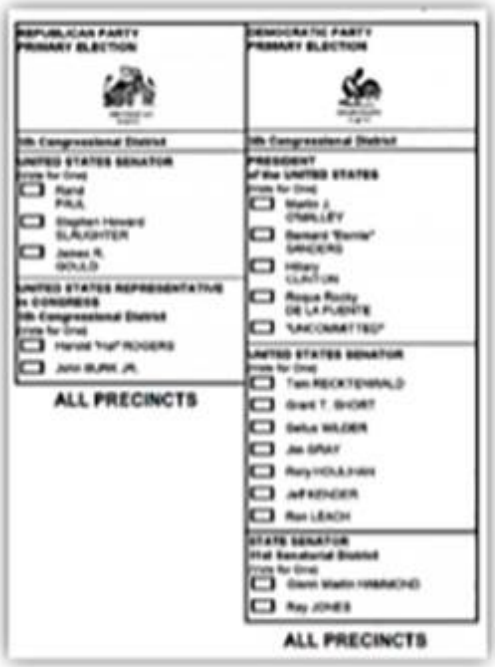
problems persist—even into the recent 2018 General Election, when a flawed ballot layout in Broward County triggered a spike in undervotes in a tight race for Senate (see the image on the next page).

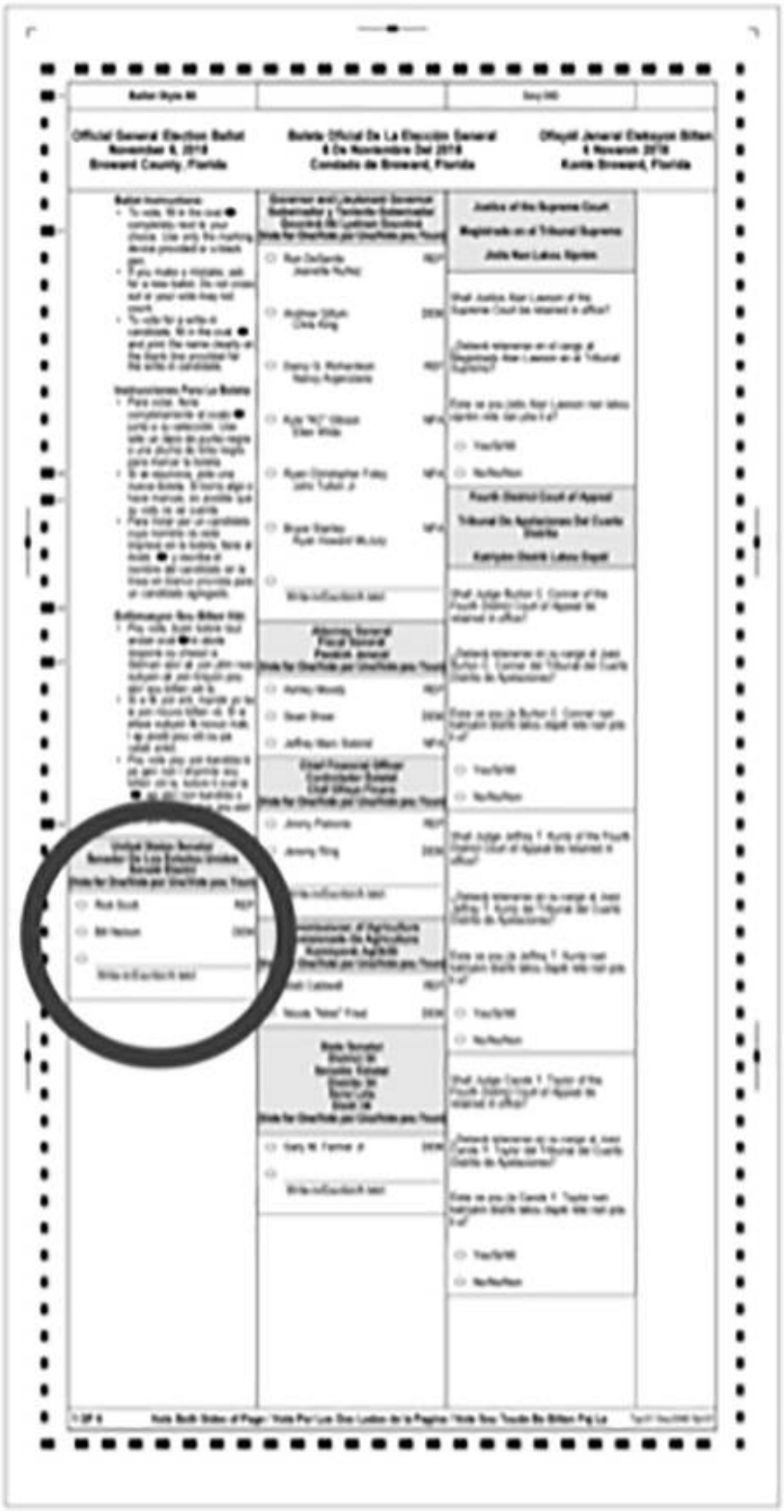
What makes this especially tragic is that we are not coming up with new problems…just new permutations of the same problems. A poorly designed ballot can result in voters making mistakes that result in a ballot that looks to be clearly marked (that is, it's been marked in an unambiguous way that the scanner easily reads) but in reality, they have not voted as they intended.

We need a better paper trail with ballots that are designed for capturing voter intent, that works for voters with the full range of civic literacy, elections savvy, physical and cognitive abilities. Ballots that don't rely on voters remembering or understanding the rules with no support from the voting system to verify their ballot. And ballots that are easy to read during an audit.

To get there, let's start with the process of voting. A ballot is the result of a conversation between the voter and the voting system to produce a paper ballot that reflects their intent with no ambiguous or inaccurate marks. We might think about ballots as a menu, showing all of the options. But when you go to your favorite restaurant, you don't order everything on the menu, so your bill at the end of the meal shows you what you selected. To make this metaphor work for a ballot, it also has to include any opportunity not taken in the list of selections.

Election history is a rogue's gallery of design defects. For more examples with the impact on real elections, see the Brennan Center's 2008 report, "Better Ballots." Left: Open primary with both parties on the same ballot. Center: Ballot with a contest split across two columns. Right: a contest in the left column, below the instructions.





The 2018 Broward County ballot, with contests below the instructions, compared to the EAC best practices and flawed Florida sample ballot. Left: The Broward County 2018 ballot. Right: Sample ballot from the EAC best practices.

Designing a voter selections ballot also requires understanding how marking a ballot moves through different information design needs for each stage of the process, in a form of progressive disclosure.

- As a voter first marks the ballot, the emphasis is on the rules and choices, helping the voter focus on each contest, one at a time.
- At the review screen of an electronic ballot marking interface, the focus shifts to a preview of all contests and selections, emphasizing missed opportunities to vote.
- Then, the printed ballot is a confirmation, with the ability to verify all of the contests and selections (and undervotes) before casting the ballot.

In addition to its accessibility features, the value of an electronic marking interface is that the voting system understands and can communicate the rules for the election: how many votes are allowed in each contest, voting variations like straight-party or ranked choice voting. It can also meet the goals of the Help America Vote Act by preventing overvotes entirely.

Seen in context, verification is not a proofreading task. It is the moment when a voter can say, "This is my ballot, and after all of the process for marking the ballot, this is how I am voting." For this moment to be meaningful, the ballot must be designed to be scanned quickly and accurately, with clear presentation of names, parties, and non-selections.

In addition to the design, the presentation of the physical ballot also matters. A piece of paper behind glass is not a useful verification artifact if voters can't read it because the text is too small, or the transport mechanism obscures part of the information, or glare from the glass makes it impossible to read. And no paper ballot supports verification for blind and low-vision voters unless is it can either be read back into a system or scanned with independent, trusted personal assistive OCR technologies.

Unambiguously marked ballots that are easy to read also have an effect on risk limiting audits. According to experts like Jennifer Morrell, much of the time in an audit is spent adjudicating voter intent on hand-marked ballots.

Because the Center for Civic Design is the voice of the humans in the process, we also have to mention the need to make risk limiting audits easy to run. Election workers need procedures, tools, and instructions that are clear, usable, and effective. There are best practices for writing good instructions for complex procedures and for designing forms. Let's bring them into election administration procedures, because elections work better when all of the materials are easy to use.

FURTHER READING

WEBSITES AND GUIDES ON ELECTION AUDITS

Lovato, Jerome. 2018. Risk-Limiting Audits – Practical Application. U.S. Election Assistance Commission.

Morrell, Jennifer. 2019. Knowing it's Right: A Two-Part Guide to Risk-Limiting Audits. Democracy Fund.

National Conference of State Legislatures. Post-Election Audits.

National Institute of Standards and Technology. Interoperability Public Working Group and Common Data Format (CDF) for Election Systems Project.

Stark, Philip. Tools for Comparison Risk-Limiting Election Audits.

Stark, Philip. Tools for Ballot-Polling Risk-Limiting Election Audits.

U.S. Election Assistance Commission. Post Election: Audits and Recounts.

U.S. Election Assistance Commission. Voluntary Voting System Guidelines.

Verified Voting. Post Election Audits.

STATISTICAL MODELS OF POST-ELECTION BALLOT AUDITING

Aslam, Javed A., Raluca A. Popa, and Ronald L. Rivest. 2008. On Auditing Elections When Precincts Have Different Sizes. Proceedings of the 2008 USENIX/ACCURATE Electronic Voting Technology Workshop.

Benaloh, Josh, Ronald Rivest, Peter Y.A. Ryan, Philip Stark, Vanessa Teague, and Poorvi Vora. 2015. End-to-End Verifiability. arXiv:1504.03778

Baxter, Patrick, Anne Edmundson, Keishla Ortiz, Ana Maria Quevedo, Samuel Rodriguez, Cynthia Sturton, and David Wagner. 2012. Automated Analysis of Election Audit Logs. Proceedings of the 2012 USENIX/WOTE Conference.

Bell, Susan, Josh Bealoh, Michael Byrne, Dana DeBeauvoir, Bryce Eakin, Gail Fisher, Philip Kortum, Neal McBurnett, Julian Montoya, Michelle Parker, Olivier Pereira, Philip Stark, Dan Wallach, Michael Winn. 2013. STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System. JETS: USENIX Journal of Election Technology and Systems, 1.1.

Cordero, Arel and David Wagner. 2008. Replayable Voting Machine Audit Logs. Proceedings of the 2008 USENIX/ACCURATE Electronic Voting Technology Workshop.

Davtyan, Seda, Sotiris Kentros, Aggelos Kiayias, Laurent Michel, Nicolas Nicolaou, Alexander Russell, Andrew See, Narasimha Shashidhar, and Alexander A. Shvartsman. 2008. Pre-Election Testing and Post-Election Audit of Optical Scan Voting Terminal Memory Cards. Proceedings of the 2008 USENIX/ACCURATE Electronic Voting Technology Workshop.

Laurent, Michel, Alexander Shvartsman, and Nikolaj Volgushev. 2014. A Systematic Approach to Analyzing Voting Terminal Event Logs. JETS: USENIX Journal of Election Technology and Systems, 2.2.

Lindeman, Mark and Philip B. Stark. A Gentle introduction to Risk-limiting Audits. IEEE Security & Privacy 10, no. 5 (2012): 42-49.

Lindeman, Mark, Philip Stark, and Vincent Yates. 2012. BRAVO: Ballot-polling Risk-limiting Audits to Verify Outcomes. Proceedings of the 2012 USENIX/WOTE Conference.

Lindeman, Mark, Mark Halvorson, Pamela Smith, Lynn Garland, Vittorio Adona, and Dan McCrea, eds. Principles and Best Practices for Post-Election Audits.

Risk-Limiting Audits Working Group. 2012 (Version 1.1). Risk-Limiting Post-Election Audits: Why and How.

Rivest, Ronald L. 2018. Bayesian Tabulation Audits Explained and Extended.

Rivest, Ronald L. and Emily Shen. 2012. A Bayesian Method for Auditing Elections. Proceedings 2012 EVT/WOTE Conference.

Shenker, Jacob, and R. Michael Alvarez. 2014. Mitigating Coercion, Maximizing Confidence in Postal Elections. JETS: USENIX Journal of Election Technology and Systems, 2.3.

Stark, Philip B. 2009. Risk-Limiting Postelection Audits: Conservative P-Values From Common Probability Inequalities. IEEE Transactions on Information Forensics and Security, Vol. 4, No. 4.

Stark, Philip B. 2012. Ballot-polling Risk-limiting Audits in Two Pages (±1).

Stark, Philip B. Tools for Comparison Risk-Limiting Election Audits. Website.

Stark, Philip B. Tools for Ballot-Polling Risk-Limiting Election Audits. Website.

Stark, Philip B. and David Wagner. 2012. Evidence-Based Elections. IEEE Security and Privacy, Special Issue on Electronic Voting.

University of Connecticut. Center for Voting Technology Research. Computer Assisted Post Election Audits. Website.

Verified Voting. Post-Election Audits. Website.

QUANTITATIVE STUDIES OF POST-ELECTION BALLOT AUDITING

Alvarez, R. Michael, Lonna Rae Atkeson, and Thad E. Hall. 2012. Evaluating Elections: A Handbook of Methods and Standards. New York: Cambridge University Press, Chapter 5.

Alvarez, R. Michael, Lonna Rae Atkeson, and Thad E. Hall, editors. 2012. Confirming Elections: Creating Confidence and Integrity through Election Auditing. New York: Palgrave MacMillan.

Alvarez, R. Michael, Jonathan N. Katz, Sarah A. Hill, and Erin K. Hartman. 2012. Machines Versus Humans: The Counting and Recounting of Paper Ballots in LA County. In R. Michael Alvarez, Lonna Rae Atkeson, and Thad E. Hall, editors. 2012. Confirming Elections: Creating Confidence and Integrity through Election Auditing. New York: Palgrave MacMillan, 73-88.

Ansolabehere, Stephen, Barry C. Burden, Kenneth R. Mayer, and Charles Stewart III. 2018. Learning from Recounts. Election Law Journal: Rules, Politics, and Policy 17.2: 100-116.

Ansolabehere, Stephen and Reeves Andrew. 2012. Using Recounts to Measure the Accuracy of Vote Tabulations: Evidence from New Hampshire Elections 1946–2002. In Confirming Elections: Creating Confidence and Integrity through Election Auditing, eds. Michael Alvarez R., Atkeson Lonna Rae, and Hall Thad E.. New York: Palgrave.

Goggin, Stephen N., Michael D. Byrne, Juan E. Gilbert, Gregory Rogers, and Jerome McClendon. 2008. Comparing the Auditability of Optical Scan, Voter Verified Paper Audit

Trail (VVPAT) and Video (VVVAT) Ballot Systems. Proceedings of the 2008 USENIX/ACCURATE Electronic Voting Technology Workshop.

Kim, Eric, Nicholas Carlini, Andrew Chang, George Yiu, Kai Wang, and David Wagner. 2013. Improved Support for Machine-Assisted Ballot-Level Audits. JETS: USENIX Journal of Election Technology and Systems, 1.1.

McLaughlin, Katherine and Philip B. Stark. 2011. Workload Estimates for Risk-Limiting Audits of Large Contests.

National Academies of Sciences, Engineering, and Medicine. 2018. Securing the Vote: Protecting American Democracy. Washington, DC: The National Academies Press.

» *Further information about the report and related resources can be found at the committee's webpage.*

Stark, Philip B., and Vanessa Teague. 2014. Verifiable European Elections: Risk-limiting Audits for D'Hondt and Its Relatives, JETS: USENIX Journal of Election Technology and Systems, 3.1.

U.S. Vote Foundation. 2015. The Future of Voting: End-to-End Verifiable Internet Voting—Specification and Feasibility Study.

CASE STUDIES OF POST-ELECTION BALLOT AUDITING

Bader, Max. 2013. Do new voting technologies prevent fraud? Evidence from Russia. JETS: USENIX Journal of Election Technology and Systems, 2.1.

California Post-Election Audit Standards Working Group. 2007. Report: Evaluation of Audit Sampling Models and Options for Strengthening California's Manual Count.

Davtyan, Seda, Sotiris Kentros, Aggelos Kiayias, Laurent Michel, Nicolas Nicolaou, Alexander Russell, Andrew See, Narasimha Shashidhar, and Alexander A. Shvartsman. 2008. Pre-Election Testing and Post-Election Audit of Optical Scan Voting Terminal Memory Cards. Proceedings of the 2008 USENIX/ACCURATE Electronic Voting Technology Workshop.

Chilingirian, Berj, Zara Perumal, Ronald L. Rivest, Grahame Bowland, Andrew Conway, Philip B. Stark, Michelle Blom, Chris Culnane, and Vanessa Teague. 2016. Auditing Australian Senate Ballots. arXiv:1610.00127

The Colorado Risk-Limiting Project. Overview.

Douglas, Michael. 2014. Ballot Bungles: Lessons from the Australian Senate. Election Law Journal 13.4: 559-569.

Hall, Joseph Lorenzo. 2008. Improving the Security, Transparency, and Efficiency of California's 1% Manual Tally Procedures. Proceedings of the 2008 USENIX/ACCURATE Electronic Voting Technology Workshop.

ELECTION FORENSICS

A. Election Observation

Bland, Gary. 2015. Measuring the Quality of Kenya's March 2013 Election. Election Law Journal 14.2: 136-147.

Hall, Joseph, Emily Barabas, Gregory Shapiro, Coye Cheshire, and Deirdre Mulligan. 2012. Probing the Front Lines: Pollworker Perceptions of Security & Privacy. Proceedings of the 2012 USENIX/WOTE Conference.

Herron, Erik S., and Nazar Boyko. 2016. Conducting Credible Elections Under Threat: Results from a Survey of Election Administrators. Election Law Journal 15.4: 285-301.

Pomares, Julia, Ines Levin, and R. Michael Alvarez. 2014. Do Voters and Poll Workers Differ in their Attitudes Toward e-voting? Evidence from the first e-election in Salta, Argentina. JETS: USENIX Journal of Election Technology and Systems, 2.2.

B. Digit Tests

Beber, Bernd, and Alexandra Scacco. 2012. What the Numbers Say: A Digit-Based Test for Election Fraud. Political Analysis 20.2: 211-234.

Deckert, Joseph, Mikhail Myagkov, and Peter C. Ordeshook. 2011. Benford's Law and the Detection of Election Fraud. Political Analysis 19.3: 245-268.

Jiménez, Raúl, and Manuel Hidalgo. 2014. Forensic Analysis of Venezuelan Elections during the Chávez Presidency. Plos One 9.6: e100884.

Klimek, Peter, et al. 2012. Statistical detection of systematic election irregularities. Proceedings of the National Academy of Sciences 109.41: 16469-16473.

Mebane, Walter. 2008. Election Forensics: The Second-Digit Benford Law's Test and Recent American Presidential Elections. In Election Fraud: Detecting and Deterring Electoral Manipulation, eds. R. Michael Alvarez, Thad E. Hall, Susan D. Hyde, 162–81. Brookings.

Weidmann, Nils B., and Michael Callen. 2013. Violence and Election Fraud: Evidence from Afghanistan. British Journal of Political Science 43.1: 53-75.

C. Quantitative Forensics

Levin, Ines, Gabe A. Cohn, Peter C. Ordeshook, and R. Michael Alvarez. 2009. Detecting Voter Fraud in an Electronic Voting Context: An Analysis of the Unlimited Reelection Vote in Venezuela. EVT/WOTE '09 Proceedings, August 10-11, 2009, Montreal, Canada.

Levin, Ines, Julia Pomares, and R. Michael Alvarez. 2012. Using Machine Learning Algorithms to Detect Election Fraud. In R. Michael Alvarez, editor, Computational Social Science: Discovery and Prediction. New York: Cambridge University Press, 266-294.

Wand, Jonathan N., Kenneth W. Shotts, Jasjeet S. Sekhon, Walter R. Mebane, Michael C. Herron, and Henry E. Brady. 2001. The Butterfly Did It: The Aberrant Vote for Buchanan in Palm Beach County, Florida. American Political Science Review 95.4: 793-810.

D. Registration Database Auditing

Ansolabehere, Stephen and Eitan Hersh. 2010. The Quality of Voter Registration Records: A State-by-State Analysis. Report, Caltech/MIT Voting Technology Project.

Brater, Jonathan, Kevin Morris, Myrna Perez, Christopher Deluzio. 2018. Purges: A Growing Threat to the Right to Vote. Brennan Center for Justice..

Norden, Lawrence. Voting System Failures: A Database Solution. Brennan Center for Justice. 2010.

Ponoroff, Christopher. 2010. Voter Registration in a Digital Age. Brennan Center for Justice.

Weiser, Wendy. 2009. Voter Registration Modernization: Collected Reports and Papers. Brennan Center for Justice.

Minneapolis
WISCONSIN
Milwaukee
Madison
Lansing
Chicago
Detroit
Cleveland
Indianapolis
IND.
Omaha
Springfield
Kansas City
St. Louis
OHIO
Baltimore
W.VA.
Charleston
Frankfort
MISSOURI
Nashville
TENN.
Charlotte
Memphis
Huntsville
S.C.
Columbia
ARK.
Dallas
MISS.
ALA.
Atlanta
Savannah
LA.
Jackson
Montgomery
Rouge
Mobile
Tallahassee
Jacksonville
Waco
New Orleans
Houston
Galveston
Lafayette
Orlando
Cape Canaveral
Corpus Christi
St. Petersburg
Tampa
Ft. Lauderdale
Miami
Grand Bahama
Great Ab
GULF OF

MIT ELECTION DATA + SCIENCE LAB

Caltech/MIT Voting Technology Project

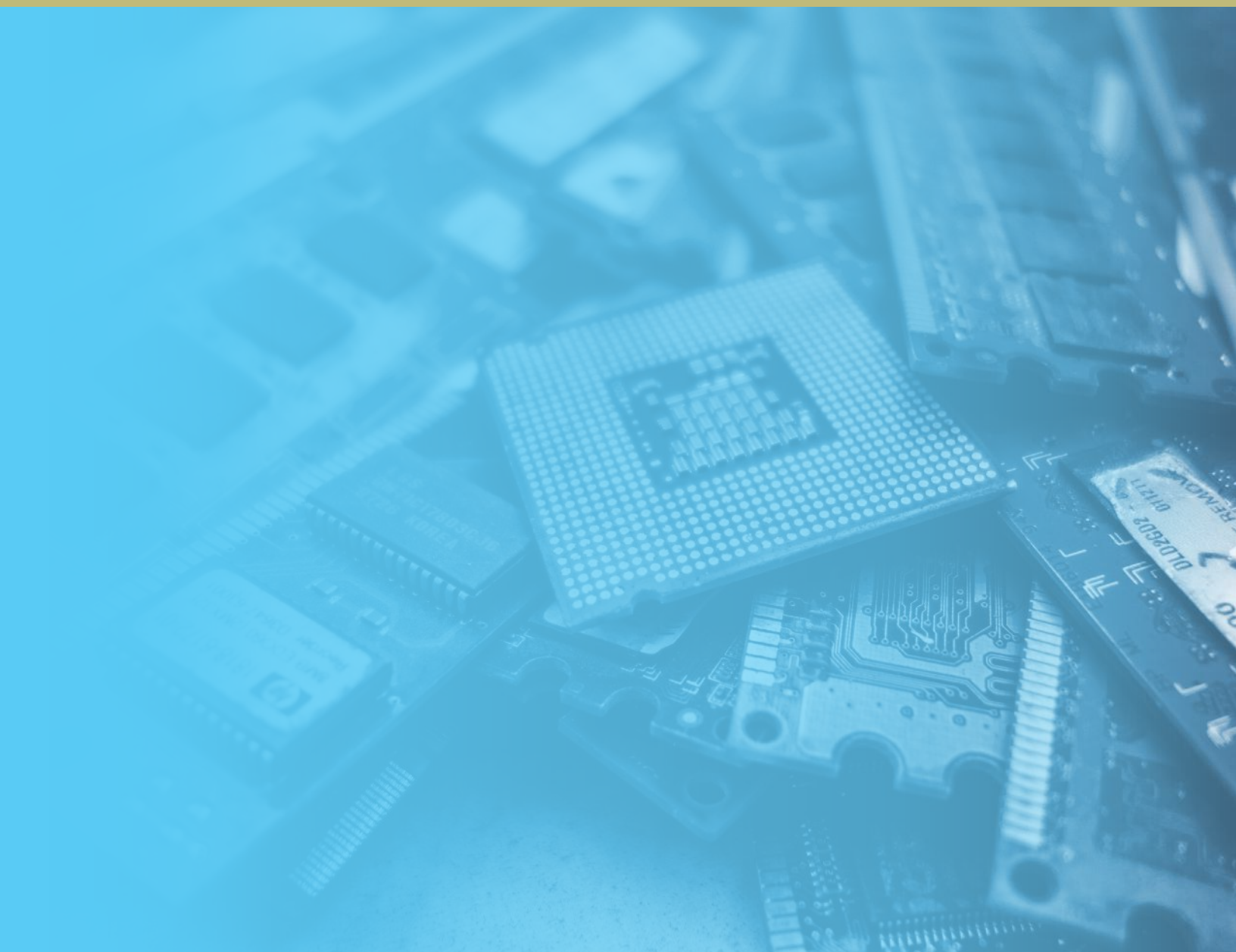


EXHIBIT 4

Declaration of Col. John R. Mills (USAR Ret.) (Nov. 21, 2021)

I, John R. Mills, declare under penalty of perjury that the following is true and correct:

1. I have personal knowledge of the matters set forth below and could and would testify competently to them if called upon to do so.

Introduction

2. I am Colonel, USAR, (Retired), John R. Mills and also Former Director of Cybersecurity Policy, Strategy, and International Affairs, Office of the Secretary of Defense, Senior Civilian (Retired). My dual career as an Active and Reserve member of the U.S. Army as well as a senior civilian in the Department of Defense has given me a unique opportunity for almost 40 years to participate directly, provide oversight, or be aware of a vast expanse of the planning and use of a wide range of U.S. cybersecurity-related instruments of national power. I have held Top Secret, Sensitive Compartmented Information (SCI) security clearances since approximately 1988. I have also been an adjunct Professor and have taught graduate level cybersecurity law and policy since 2013 at the University of Maryland, Global Campus. My last uniform position in the Department of Defense was in Homeland Defense and I often served as a liaison with Department of Homeland Security to coordinate the national response to complex emergencies and threats to the Homeland (real events and exercises).

3. I have been asked to testify on the development, capabilities, and uses of "remote access operations" for unlawful entry and purposes into networks. The information presented is unclassified and based upon my personal experiences, publicly available reporting, studies, events, incidents, best practices, and de-classified U.S. Government information. Remote access operations for nefarious purposes refer generally to the methods and activities used to access networks, data centers, and other

locations, often enabled by planted malware, enabling software, and/or algorithms, conducted in a manner to avoid detection or leaving behind of identifying forensic evidence of penetration.

4. Remote access operations are different than remote maintenance monitoring which is intended by network designers for transparent and auditable access to network enabled devices for maintenance and updates. Remote maintenance monitoring can also be employed or co-opted for reasons not in accordance with remote maintenance monitoring tenets, design intent, network owners/operators, or lawful access/purpose. Electronic election infrastructure is just one example of critical infrastructure which can be subjected to remote access operations. The U.S. Government conducts remote access operations through the entities described in Executive Order 12333[1], as described in the articulation of the U.S. Intelligence Community (IC)[2] roles, missions, and organization, and as directed by a sitting President (POTUS). The IC is also enabled by and often operates in close coordination with the Department of Defense and Federal Law Enforcement for these operations.

5. In addition, other countries, organizations, and individuals have also developed these remote access capabilities with varying degrees of sophistication. Such capabilities have been expanding at an accelerating rate in the past 20 years threatening critical infrastructure, such as election systems[3], in ways that threaten the very foundation of our Republic i.e. the foundational tenet that leaders in our Country are actually chosen by the People through a voting system based on "one person one vote" as opposed to an election system that is compromised by malign actors seeking to exploit an election for their own benefit.

---

[1] Presidential Executive Order 12333 United States Intelligence Activities (As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008));
https://irp.fas.org/offdocs/eo/eo-12333-2008.pdf

[2] EPIC.org, "Background on Executive Order 12333"; https://archive.epic.org/privacy/surveillance/12333/

[3] CISA Website, Election Infrastructure as Critical Infrastructure, https://www.cisa.gov/election-security

6. The employment of machine-based algorithms accessing electronic voting systems in the United States to attempt to achieve a pre-determined election outcome through remote access operations is well within the capabilities of many nation-state actors such as China, Russia, Iran, and Venezuela, as well as even non-nation state actors.

7. From the 1980s to the present, the capabilities, scope, and scale of remote access operations to collect or alter data have greatly expanded in their scale, access, and ability. These operations have become ubiquitous through nation state and private actors. The offense in remote access operations normally has a decided advantage against defenders.

Summary of Findings

8. The U.S. Government has pioneered and pushed the envelope on the art and techniques of remote access of critical infrastructure.

9. Based on my personal experience the United States Government has the capability to project significant effects[4] toward critical infrastructure worldwide—including election systems—if a complete decision process up to and including the President was conducted and completed. This same capability (to project effects) now exists in other countries, such as China, Russian, Iran, and Venezuela, and these foreign powers now use these same, similar, and improved remote access operation methodologies at will to assert their own national agendas.

10. These operations have created a growing talent base of personnel, software, and network enabled capabilities that are becoming ubiquitous in the hands of companies and personnel outside of the U.S. Government.

---

[4] "Effects" is an operator's and planner's term of art which implies the ability to degrade, exfiltrate, manipulate, change, or destroy.

11. The U.S. Government made strong statements on the maturity level of U.S. Government capabilities regarding election security during the November 2020 election. With my professional experience and my understanding of the election process in America (I have not yet found a U.S. Government national security professional who has also participated as a sworn election official and demonstrates an understanding of the election process at the county level), I have very low confidence in the security of American election critical infrastructure. In my professional opinion, assertions by the IC, Homeland Security, and other law enforcement officials that they have the situational awareness and capability to defend these environments, including the election environment as part of national critical infrastructure with a high level of confidence are unsupported and, in some cases, may be false. Several publicly known breaches of critical infrastructure are presented later in this document and one of the most damaging and egregious was the breach of the Office of Personal Management which created catastrophic results. The full resources and full spectrum of the U.S. Government were available to detect, prevent, stop, mitigate, or otherwise address the attack on this critical infrastructure, yet that is not what happened.

12. My professional opinion is that the statement "The November 3rd election was the most secure in American history" asserted in a November 12, 2020, posted on the Cybersecurity and Infrastructure Security Agency ("CISA") website, had little, if any, basis in fact.[5]

13. Moreover, in my professional opinion, the assertions by then-Director of CISA, Christopher Krebs, claiming the November 2020 election was secure had similarly little, if any basis in fact. Indeed, Mr. Krebs largely refuted his own November 2020 comments in his February 10, 2021,

---

[5] CISA, Joint Statement, November 12, 2020, https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election

testimony to Congress[6], and gravely injured his and the CISA's credibility on delivering a secure environment for the election systems employed in the United States.

14. In my professional opinion, based upon substantial experience on national cyber capabilities, cybersecurity, planning, policy, strategy, and with my knowledge of the election process, the statements made by CISA and Krebs referred to above, to be properly, independently, and holistically assessed must include a factual establishment and public release of the actual National Intelligence Collection priorities at the time of the November 2020 election, and the precise and specific signatures and indicators the national intelligence collection system (and law enforcement), and their capabilities were supposedly tuned to monitor, collect, and defend the 2020 election[7]. The broad assertions and statements by Mr. Krebs and others also presume an ability to detect these remote access operations in an extremely timely manner with extremely high confidence—which is simply not realistic at this point in time and have a poor track record.

Relevant Experience and Qualifications of Author

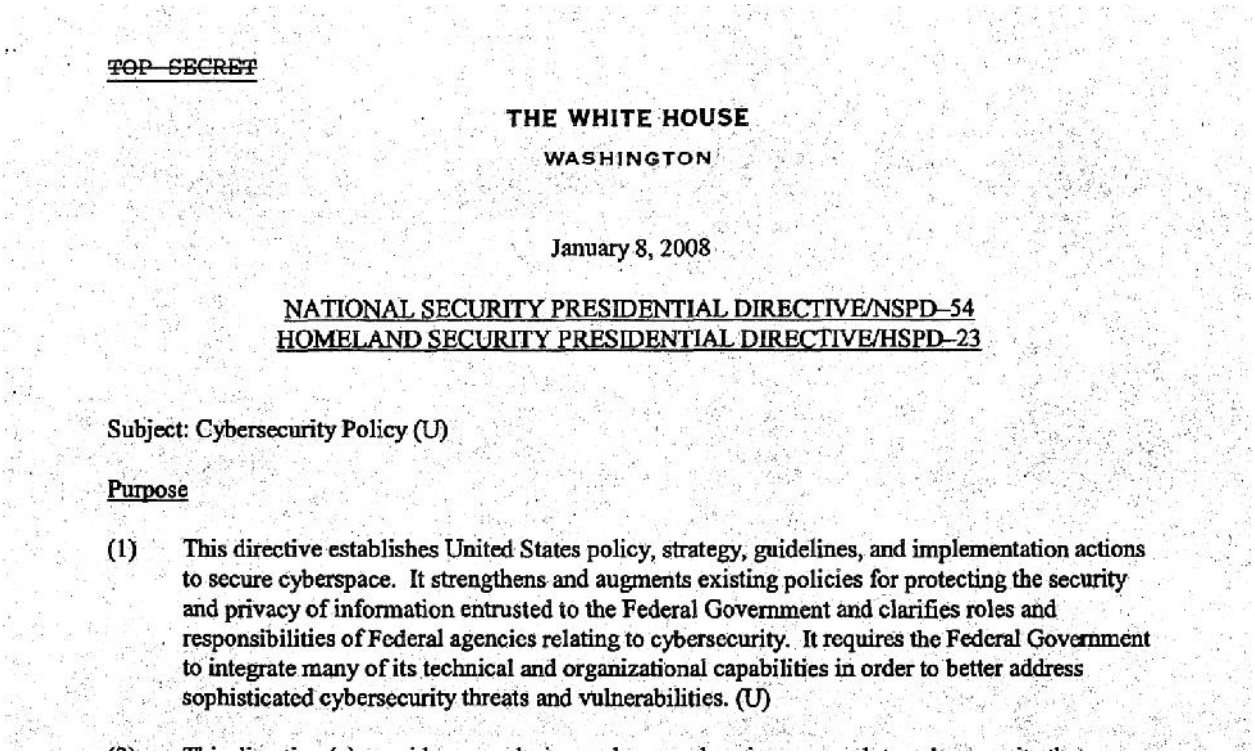
15. I have defended our Country since 1983. My service for our Nation ranges from the tactical level in combat to the strategic at the Office of the Secretary of Defense (DOD). I am a school trained and qualified Military Intelligence Officer, Psychological Operations Officer (PSYOP – a Special Operations Community Branch), Civil Affairs Officer (also a Special Operations Community Branch), and Public Affairs Officer. My role has essentially been as a national security strategic planner since approximately 2001. My service at the senior levels of the U.S. Government has included: complex inter-agency proceedings and deliberations on cyber and cybersecurity and other whole of government

---

[6] Christopher Krebs Testimony Committee on Homeland Security, February 10, 2021 https://docs.house.gov/meetings/HM/HM00/20210210/111152/HHRG-117-HM00-Wstate-KrebsC-20210210.pdf

[7] The code name of the operation(s), their planning documents, establishment of inter-agency roles and missions, and all coordinating instructions to include the detailed guidance on factual Intelligence Collection priorities, including signatures and indicators, must be made public.

operations across the whole spectrum of instruments of national power; international partner negotiation of sensitive information sharing agreements (including the Five Eyes (FVEYS[8])); and being the DOD representative at the National Security Council from mid 2008 to mid 2009 as NS/HSPD-54/23[9] when the Comprehensive National Cybersecurity Initiative (CNCI)[10] was brought to life as described in following official memorandum (a formal Presidential Directive of the President George W. Bush Administration).



~~TOP SECRET~~

THE WHITE HOUSE

WASHINGTON

January 8, 2008

NATIONAL SECURITY PRESIDENTIAL DIRECTIVE/NSPD–54
HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD–23

Subject: Cybersecurity Policy (U)

Purpose

(1) This directive establishes United States policy, strategy, guidelines, and implementation actions to secure cyberspace. It strengthens and augments existing policies for protecting the security and privacy of information entrusted to the Federal Government and clarifies roles and responsibilities of Federal agencies relating to cybersecurity. It requires the Federal Government to integrate many of its technical and organizational capabilities in order to better address sophisticated cybersecurity threats and vulnerabilities. (U)

Figure 1: NS/HSPD-54/23

[8] "The Five Eyes was formally founded in the aftermath of the Second World War, through the multilateral agreement for co-operation in signals intelligence (SIGINT), known as the UKUSA Agreement, on 5 March 1946." Since this original agreement, Canada, Australia, New Zealand have been added as well as other countries for unique functional topics. https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/

[9] Department of Homeland Security, Fact Sheet: Preventing and Defending Against Cyber Attacks, October 18, 2011; https://www.dhs.gov/news/2011/10/18/preventing-and-defending-against-cyber-attacks

[10] FAS.ORG; De-classified Text of HS/NSPD-54/23: Cybersecurity Policy; https://irp.fas.org/offdocs/nspd/nspd-54.pdf

Signed January 8, 2008, by President George W. Bush

16. CNCI represented a large-scale leap ahead in Cybersecurity of the American nation state as the title implies, but also developed significant new remote access capabilities submerged inside the program. Portions of paragraph 47 of the CNCI document (pages 12-13) are partially redacted and possibly point to additional capabilities. In layperson's terms, robust remote access operations can range across several functional activities and can possibly include exfiltration or manipulation of data on a large scale of critical infrastructure —including electronic voting systems. NS/HSPD-54/23 was a defining event in the history of U.S. Government remote access operations. The CNCI effort was a disruptive, historical inflection point for collection of information on a massive scale never seen before. From 2007 forward, the ability to penetrate networks, and manipulate or gain information on scale, expanded exponentially.

17. In both my uniformed service, civilian service, and post-U.S. Government service I have had several unique opportunities to work, plan, implement, observe, and make recommendations in both American elections and foreign elections. I have been a sworn election official in my home county, Prince William County Virginia, multiple times since the early 2000s, including the November 2020 election. Day of voting was almost irrelevant in my county. 74% of the votes in the November 2020 election were absentee in one of several forms. This meant that 74% of the ballots were handled at what is known as the Central Absentee Precinct (CAP), a first in Virginia and handled with very unclear guidance on chain of custody for thumb drives removed and moved around with little chain of

custody procedures. The use of a thumb drive is a key enabler in cyber intrusions based upon the Agent BTZ[11] and possibly Stuxnet[12].

18. While in uniform I have been personally responsible for information campaigns communicating the importance of a transparent and trustworthy election process and the compelling imperative of citizen involvement. This was during my service in Bosnia in 1997. In addition, I participated in the establishment of a clean election process in Iraq which was one of the first strategic imperatives in the post regime change environment. From 2003 to approximately 2009, I was routinely part of meetings and projects from the tactical to the Combatant Command, to the strategic level where issues, themes, processes, and conduct of elections in Iraq were discussed and formulated.

19. Out of office, I was asked for my actionable recommendations for the January 2020 elections in Taiwan. I made two basic recommendations. The first was the necessity for a new, national security law, prohibiting the acceptance of foreign money regarding elections in Taiwan. My second recommendation was to make the process as simple and transparent as possible and the critical importance of official ballot standards and the use of the "dumbest and simplest" ballot tabulation machines possible. The machine should have no other feature other than to simply tabulate the ballot. Such a configuration limits remote access operations to unique access methods such as 110- or 220-volt power cords (i.e., wall power that the machine is plugged into)[13]. The machines should have no features other than simple tabulation and should have no connectivity sub-components such as Bluetooth, modems, or anything else. Simply put, the Taiwanese executed flawlessly. A new law was

---

[11] Council on Foreign Relations, Cyber-Operations, "Agent.btz", November 2008 https://www.cfr.org/cyber-operations/agentbtz

[12] CNET, Stuxnet delivered to Iranian nuclear plant on thumb drive", April 12, 2012, https://www.cnet.com/news/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/

[13] The Hacker News, "Hacker can steal data from air-gapped computers through Power Lines, April 12, 2018, https://thehackernews.com/2018/04/hacking-airgap-computers.html

passed[14], arrests were made of foreign influence operatives, and the election was conducted in a model of transparent processes using manual processes to the greatest extent possible, enabled by the simplest of election machines and technology. The outcome was magnificent and Chinese influence operations to throw the election were crushed.

20. In all my election work as an American sworn election officer in U.S. elections, in Bosnia and Iraq as a Uniformed Military Officer and senior civilian, and assessment of Taiwan elections as a private citizen (advice rendered to other American nationals), we have either been trained, told, looked to, or were supposed to abide by the principles of the Carter Center for Democracy, and their recommended best practices for free and fair elections. The Carter Center Manual, Chapters 8 – 10[15] are considered the gold standard in the conduct of democratic elections. In my professional opinion, American elections deviate substantively from the best practices endorsed by the Carter Center. Just a few of the examples include:

a. Right of the State to determine and enforce citizenship for voting (P.147): In Virginia I identified 8 -12% of registered voters in my county were unlawful based on 2019 rejection of voters for jury duty. There was no action by my Election Registrar or Board after being presented this apolitical, factual evidence.

b. Independent Body to review electronic voting technologies (P.152): There is no pervasive implementation of qualified independent bodies provided with uniform minimum standards at the county or state level to review election technologies that I am aware of. Currently, county election personnel cede sovereignty on all election technologies to their contractors. I have never come across a county situation where the sworn election officials know how to access or see network activity

---

[14] ABC News, "Taiwan passes law targeting Chinese Political Interference, December 31, 2019, https://abcnews.go.com/International/wireStory/taiwan-passes-law-targeting-chinese-political-interference-67996333

[15] The Carter Center, "Election Obligations and Standards"; https://www.cartercenter.org/resources/pdfs/peace/democracy/cc-OES-handbook-10172014.pdf

beyond the machine. There is no independent, 3rd party verification and validation I have ever come across. Contractors will often assert intellectual property rights or contractual terms and conditions to deny any third-party review of the network/cloud environment beyond the election machine. For example, it has been publicly reported that "a software update [was] installed to address a glitch in Georgia's voting machines" just a few weeks prior to the November 2020 election.[16] It does not appear that this "update", and it's purpose or effect, was ever reviewed by any qualified independent bodies in that State."

c. Unfettered observation of the election process (P.155): There were hundreds of affidavits submitted by election poll watchers attesting to being harassed, blocked, and excluded from observing the election process. Two examples are the reports from the Philadelphia Convention Center and the Detroit TCF Center during and after the November 2020 election.

d. Judicial reviews of the election process (P.257): Up to this point in time, the judicial branch has largely deferred on in-depth reviews of the election process and has largely asserted lack of standing from any group seeking election review or recourse.

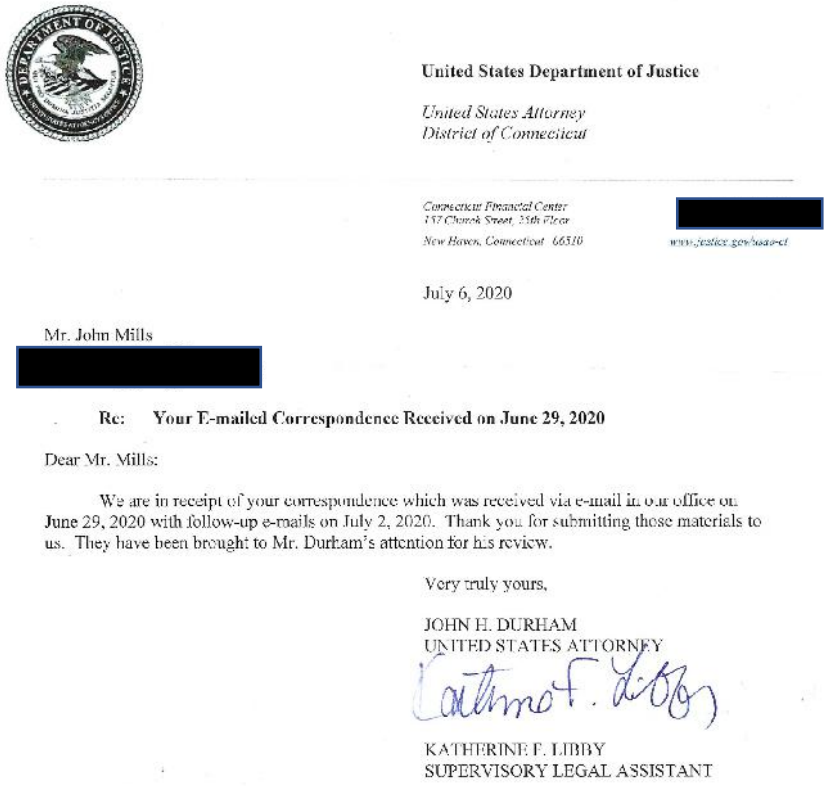
21. There is also a possible intersection between the expanding remote access operations and capabilities with the spying effort directed toward President Trump in 2016. I also was present and a witness to several events in what has become known as "Spygate" or "Russiagate". Within days of the November 2016 election, I was asked to participate in urgent inter-agency meeting to produce a Russian connection narrative, through the finalization of an Intelligence Community Assessment (ICA) which has now been established as being composed of false statements[17] from Mr. John Brennan and

---

[16] AP News, "With time short, judge mulls Georgia voting system changes", October 7, 2020, https://apnews.com/article/technology-senate-elections-georgia-elections-voting-machines-6a6be19f168a719e68c107c7426df9f3

[17] Cornell Law; 18 U.S. Code § 1001 - Statements or entries generally; https://www.law.cornell.edu/uscode/text/18/1001

Mr. James Comey. I have presented extensive evidence to U.S. Attorney for Connecticut, Mr. John Durham chronologizing these events.



United States Department of Justice

United States Attorney
District of Connecticut

Connecticut Financial Center
157 Church Street, 25th Floor
New Haven, Connecticut 06510

[redacted]

www.justice.gov/usao-ct

July 6, 2020

Mr. John Mills
[redacted]

Re: Your E-mailed Correspondence Received on June 29, 2020

Dear Mr. Mills:

We are in receipt of your correspondence which was received via e-mail in our office on June 29, 2020 with follow-up e-mails on July 2, 2020. Thank you for submitting those materials to us. They have been brought to Mr. Durham's attention for his review.

Very truly yours,

JOHN H. DURHAM
UNITED STATES ATTORNEY

KATHERINE F. LIBBY
SUPERVISORY LEGAL ASSISTANT

Figure 2: Mr. Durham Receipt of 27 Pages of names and events from Colonel (Ret) John Mills

An important attribute of the contemporary national security culture is a strong influence for conformance to an established narrative – this behavior undermines original thought, analysis, and innovation

22. In my professional experience, there often is a monoculture of singular narratives in the national security world that are established and rarely, if ever questioned, challenged, or further investigated. I have experienced this mentality in countless senior level meetings within the Pentagon, the Inter-Agency, and the White House. However, it appears that under President Trump, this strong conformance to a singular narrative changed to include outright hostility to the notion that China interfered in the November 2020 election. On January 7, 2021, the Director of National Intelligence

("DNI") concluded in an unclassified memorandum that "CIA Management took actions 'pressuring [analysts] to withdraw their support" for findings regarding China's actions to "interfere" in the election. [18] The DNI concluded that the CIA's actions violated Intelligence Community Tradecraft Standards.

The history and evolution of U.S. Government remote access operations

Compelling need for access to denied areas containing foreign actors with nuclear weapons

23. Since the Second World War and the 1947 and 1949 National Security Acts[19], the IC and the rest of the United States Government have rightly and assertively sought to attain access to denied areas[20] to defend the United States from the existential threat of the Soviet Union and others since the Second World War. The U-2, SR-71, the Corona Program[21], are but a few of the manifestations of grand and bold innovation to seek access to the true status, capabilities, and intent of a closed, secretive, and paranoid, totalitarian system with nuclear weapons at the ready to destroy the United States.

Era of Dial Up

24. In the early days of network connectivity which trace their lineage from the ARPANET[22] (Advanced Research Project Agency Network), original packet switching was often conducted through the common term of "dial up". The basic thesis was creating a resilient network for continuity of

---

[18] DNI John Ratcliffe Memo, January 7, 2021; Views on Intelligence Community Election Security Analysis; https://context-cdn.washingtonpost.com/notes/prod/default/documents/6d274110-a84b-4694-96cd-6a902207d2bd/note/733364cf-0afb-412d-a5b4-ab797a8ba154.#page=1

[19] DNI, "National Security Act of 1947", https://www.dni.gov/index.php/ic-legal-reference-book/national-security-act-of-1947

[20] Denied areas meaning totalitarian nations with hostile intent and an inability of the United States to obtain information on motives, agendas, and intent by traditional statecraft.

[21] National Aeronautics and Space Administration, "Corona"; https://space.jpl.nasa.gov/msl/Programs/corona.html

[22] Defense Advanced Research Projects Agency, "ARPANET"; https://www.darpa.mil/about-us/timeline/arpanet

communications during a nuclear exchange between the Soviet Union and America. In these early days of modern cyber (approximately 2007 being the critical year with CNCI, thus the BC/AD of cyber), computers and our personal computers had to reach out through common, copper, phone lines to knock and handshake in an analogue manner and establish a connection with another computer. During those days, it was a simple way to connect. There were no firewalls, gateways, or cybersecurity. There really was no thought to security at the time[23]. The thought of a non-compliant or hostile participant was not really considered. Why would anyone be malign?

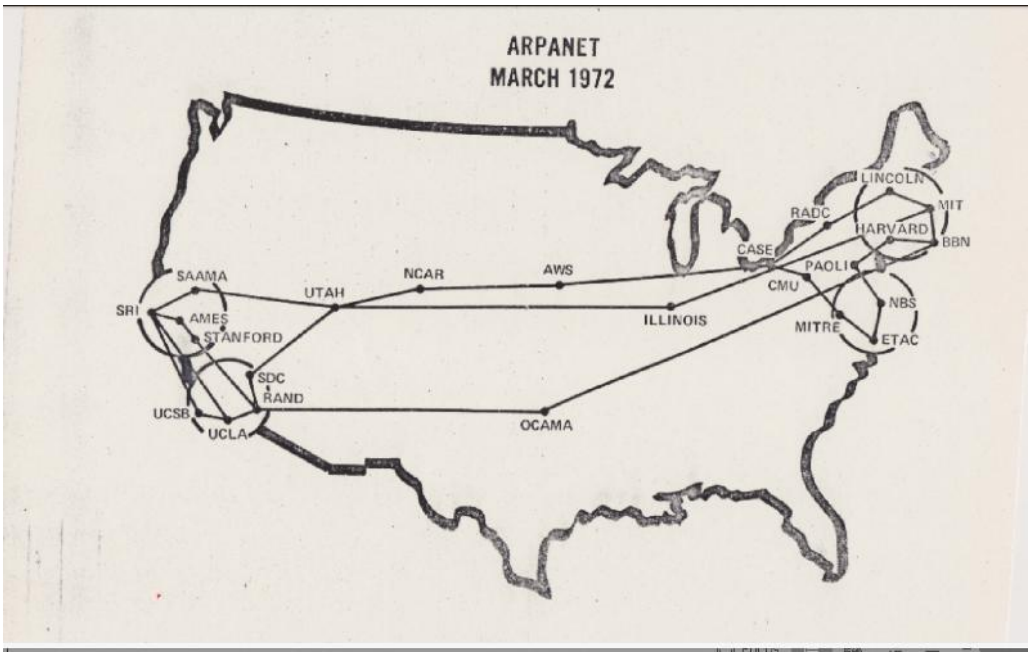


Figure 3: The original ARPANET network

[23] Washington Post, "Net of Insecurity", May 30, 2015; https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/

Major cyber intrusions enter the picture

25. As we now know, there are malign actors[24], many of them[25]. The threat actors have evolved since the early days where information technology engineers created worms[26] out of curiosity and early compartmented U.S. Government activities, possibly in participation with our Five Eyes (FVEYS) partners[27], began to poke, peek, and even fiddle with foreign networks and the Soviet Union and others did it right back.

26. In the 1980's the original concept of ARPANET began exponentially expanding, and threat actors (and American U.S. Government activities) began to realize the exploitation (i.e., exfiltrating or taking data from someone else) or mayhem they might be able to inflict on large scale. Much of the activity centered on intercepting and decrypting message traffic, but there also was deep interest and grave concern over the sanctity of our nuclear command and control systems. The CIA and NSA entered this world as well as the Department of Justice and the Federal Bureau of Investigation. The seminal statute in prosecuting computer intrusions was, and still is the Computer Fraud and Abuse Act (CFAA 18 USC 1030) from 1986[28], which gave DOJ lawyers[29] the foundational law to indict, charge, and prosecute computer crimes. The Soviet Union was the main nation state concern, China was silently organizing for the long game, non-nation state actors sometimes called "hacktivists" and organized crime were also beginning to learn, study, and exploit the rapidly developing internet.

---

[24] Cybercrime Magazine, "The History of Cybercrime And Cybersecurity, 1940 – 2020", November 30, 2020; https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/

[25] Center for Strategic and International Studies, "Significant Cyber Incidents"; https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[26] Norton, https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html

[27] Privacy International, "Five Eyes"; https://privacyinternational.org/learn/five-eyes

[28] Cornell Law School, "18 U.S. Code S. 1030 – Fraud and related activity in connection with computers"; https://www.law.cornell.edu/uscode/text/18/1030

[29] Department of Justice, "Prosecuting Computer Crimes"; https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

The visionary wisdom of Richard Clarke (and others) – but also the foundation for mass surveillance

27. Seminal national security visionary, Richard Clarke[30] began to understand the macro trend that while the American Government was establishing dominance in network enabled military warfare and intelligence collection as decisive Instruments of National Power, other forces were simultaneously exploiting our own networks.

28. Richard Clark along with others such as Admiral (Ret) Mike McConnell[31], and General (Ret) Mike Hayden[32] worked to develop the National Strategy to Secure Cyber Space[33]. This White House issuance in 2003, released while American and international partner forces were in Iraq to oust Saddam Hussain, established the future of both securing our networks and simultaneously ensuring decisive American freedom of movement at will through all other networks and the cyber environment. As with most unclassified, public facing national security issuances, there is normally voluminous Top Secret and compartmented activity behind such an issuance. The public facing document is merely the very tip of a much larger, concealed behemoth.

29. People, programs, and resources were being assembled, en masse to assert this 2003 strategy. In 2005, Secretary of Defense Donald Rumsfeld tasked General (GEN) James Cartwright, the Commander of Strategic Command, to establish the Joint Functional Component Command Network Warfare (JFCC-NW). GEN Cartwright turned around and tasked the NSA Director, Lieutenant General (LTG) at the time, Keith Alexander, to establish this entity.

30. In my office in the Pentagon, I established, what I called, my "Seminal Stack of Stuff" of documents, where I placed documents, I innately sensed as having enduring value, and placed hard

---

[30] Middle East Institute, "Richard A. Clarke"; https://www.mei.edu/profile/richard-clarke
[31] University of South Florida, "Former National Security Agency Director to lead Cyber Florida at USF"; https://www.usf.edu/news/2020/cyberflorida-gets-new-director.aspx
[32] National Security Institute, "General Michael Hayden (RET.)", https://nationalsecurity.gmu.edu/general-michael-hayden-ret/
[33] The White House, "The National Strategy to Secure Cyberspace", https://georgewbush-whitehouse.archives.gov/pcipb/

copies of them there, in addition to electronic storage. The three memos documenting the JFCC-NW arrangement were immediately placed into this stack. These documents were retrieved numerous times in the subsequent years, by myself, or my staff as core, historical artifacts for many more, future, follow-on branches, and sequels. Over the years, the "Seminal Stack of Stuff" grew voluminously.

31. All this work was the foundation of remote access at a massive scale – some of which overwhelmed, skirted, or was complicit with murkiness of the Foreign Intelligence Surveillance Court (FISA)[34] process. I knew and trusted many of the leaders overseeing these operations at the time but was also disturbed to find out later about the participation of some of these trusted, senior leaders in nefarious palace intrigue that leveraged these capabilities for personal political agendas. For example, in early 2018, General (Ret) Hayden sat 24 – 36 inches away from me coordinating his daily talking points in his almost daily phone call with James Comey, John Brennan, and others in their coordinated efforts to topple President Donald J. Trump.

32. The establishment of a mass remote access operations, while originally well intended, has now been rotated around to point at the American People. In 2010, the Washington Post presented a multi-part series entitled, "Top Secret America"[35]. We chuckled openly in Top Secret White House meetings and joked, "Well thank God they didn't find out about super double Top-Secret America" The Washington Post was on to something but didn't totally understand what they were seeing through the very foggy, windowpane.

Role of Remote Access Operations in dealing with dangerous regimes

33. Going a bit backwards to the immediate post 9/11 era, as we consolidated Coalition gains in Afghanistan, the American Instruments of National Power began to pivot and focus on chasing Al

---

[34] Foreign Intelligence Surveillance Court; https://www.fisc.uscourts.gov/

[35] Washington Post, "Top Secret America", July 21, 2010; https://www.washingtonpost.com/investigations/top-secret-america/2010/07/21/secrets-next-door/

Qaeda (AQ) throughout the world and working to factually establish the connectivity between AQ and Saddam Hussein – which was manifested in one trail by Abu Musab Al-Zarqawi (AMZ)[36]. In 2002, as AQ dispersed across the world from Afghanistan, one place some went to was Yemen. It was my Special Operations staff officer duty at this time, in the Chairman of the Joint Chiefs of Staff, J-3 Special Operations Division, to run a staffing action to resolve legal concurrence and recommend POTUS level approval and directive authority to eliminate an AQ cell in Yemen[37]. The gravity and scope of this action was immense, and it was my job, when necessary, be the scribe, negotiate, advocate, and receive the highest-level input for Secretary of Defense deliberation in the inter-agency on behalf of our immediate General, Stanley McChrystal[38], who will intersect again, later in this overview of remote access operations.

34. What does the Yemen event have to do with U.S. Government Remote Access Operations of critical infrastructure? A lot. Everything we knew on tagging, tracking, and locating these personnel with precision was based on the ability to establish remote access, full spectrum presence and dominance in all forms of critical infrastructure communications, networks, emissions, and signatures around the world. Part of this presence was the ability to deliver offensive, defensive, and exploitation effects. This nascent methodology worked, but it was labor and resource intensive, quite manual, and lacked automation to do this with multiple target tracks simultaneously.

35. In other words, presuming high precedence in the National Intelligence Collection priorities system, it could be done, but not on scale (scale meaning managing tens and hundreds of thousand simultaneous surveillance operations, not dozens. In IC idiom – moving out of the "hobby-shopped" micro-tailored solution culture of the IC, to surveilling at an exponential scale). This event was in the

---

[36] CRSR Report, "Al Qaeda in Iraq; Assessment and Outside Links", August 15, 2008; https://www.everycrsreport.com/reports/RL32217.html

[37] Journal of Conflict & Security Law, "'Targeted Killings' in an age of Terror: The legality of the Yemen Strike", Summer 2004; https://www.jstor.org/stable/26294308

[38] McChrystal Group; https://www.mcchrystalgroup.com/I

direct lineage of capabilities that led to remote access operations on scale as a normalized event. It was an iterative learning process and over time, this strategic reach became more routinized, efficient, and ubiquitous with greater numbers of personnel involved, but also with a dizzying exponential increase in "points of presence" (where information was gathered from) and simultaneous remote access operations. Conformance to law and mission guidance regarding civil liberties was being outpaced by the capability to conduct these remote access operations.

36. The intent of remote access operations was to establish full spectrum dominance of all forms of communication, information technology, and cyber in and around Iraq to project effects. Were these effects used to influence elections? According to a Foreign Affairs article[39], it was discussed but ultimately not implemented according to those interviewed. The wording in the article implies in my opinion, a declination of President Bush to approve a covert finding for the CIA to directly engage on the election and perhaps the direct method of manipulating vote tallies.

37. As time went on in Iraq and chaotic civil war broke out among several factions, we attempted different lines of effort to help establish civil society. Part of this was efficiently generating and delivering cyber effects into Iraq and relevant areas outside of Iraq. This was a complex inter-agency effort that revealed the conundrum between sharply focused and tailored Title 50 activities vis a vis the desire of Title 10 forces to conduct these operations on a much broader and routinized scale. These two different perspectives are a normal point of friction between these two worlds. At that time, Jen Easterly, now the Director of CISA at the Department of Homeland Security (DHS) appeared to have been a staff officer associated with the Tailored Access Office (TAO) of the National Security Agency (NSA) and was a key planner and integrator of the projection of capabilities. General Stan

---

[39] Foreign Affairs, "When the CIA Interferes in Foreign Elections A Modern-Day History of American Covert Action" June 21, 2020

McChrystal, who was now with the Joint Special Operations Command (JSOC) refined the art form of integrating Remote Access Operations to directly support his Commander's objectives.

38. I was working in this architecture of Military staffs, processes, and units as both a Joint Staff J-5 Middle East Staff Officer as well as an Office of the Secretary of Defense (OSD) Senior Civilian ensuring the achievement of national objectives as well as the deliberations to develop and approve the Execution Order for Countering the Adversary Use of the Internet ("CAUI,").[40], These efforts encapsulated the operational and directive authority for a family of worldwide remote access operations as well as what would become PPD-20[41] (the actual Top Secret PPD-20 may be on the internet, courtesy possibly of Edward Snowden), a follow on authority for the use of remote access operations which, in theory made the authority and approval of remote access more agile and responsive to a greater spectrum of senior leaders.

39. In a curious harbinger of issues with the 2020 election, retired General McChrystal made puzzling comments in May 2020 about his intent to use technology from this era[42], in coordination with the Lincoln Project to help ensure President Trump did not win the November 2020 election. This immediately received my attention and concern. His May 2020 announcement did not appear to receive much attention in the media. In my mind I had immediate questions – just what technologies? Were these remote access technologies from the Iraq era or beyond? Were these technologies lawfully obtained and used? Who was helping General (Ret) McChrystal? A retired General announces his intent to use US Government developed capabilities to influence a Presidential election and there is

---

[40] Committee on Armed Services, U.S. Senate, "Foreign Cyber Threats to the United States", January 5, 2017; https://irp.fas.org/congress/2017_hr/cyber-threats.pdf

[41] Executive Office of the President, "Fact Sheet on Presidential Policy Directive 20", January 2013; https://irp.fas.org/offdocs/ppd/ppd-20-fs.pdf

[42] Washington Post, "Technology once used to combat ISIS propaganda is enlisted by Democratic group to counter Trump's coronavirus messaging", May 1, 2020; https://www.washingtonpost.com/politics/technology-once-used-to-combat-isis-propaganda-is-enlisted-by-democratic-group-to-counter-trumps-coronavirus-messaging/2020/05/01/6bed5f70-8a5b-11ea-ac8a-fe9b8088e101_story.html

little intellectual curiosity from media or "experts" in the field? He certainly wasn't going to conduct these technical remote access-like operations personally. Exactly how were these capabilities going to be used and just how was he going to use them lawfully now that he was a private citizen running a private business?

40. This is one of many examples of the blurring of trained cyber personnel in government service, or under contract to the U.S. Government and the transition of this government developed tradecraft[43] for uses outside of statute-based activities. This work is supposed to be classified and controlled. Yet this transfer, seepage, and escapage is not an uncommon thing. Any use of these capabilities could implicate federal law starting with the CFAA. Nothing here made sense to me, despite a compelling obligation for the Department of Justice to issue a referral to the FBI to investigate a retired being in possession of software and technical access capabilities.

41. Sharyl Attkisson has had to deal with this as ex/former FBI personnel like Shaun Bridges[44] have allegedly used remote access capabilities developed in-house, in post government service. A culture of remote access capabilities has now become ubiquitous and perhaps commoditized. What was nurtured in classified environments has escaped, one way or another, into the wild.[45]

42. There is distinct mimicry of American efforts by great power competitors, China and Russia, and their sidekicks of Iran and Venezuela. From my almost 40 years of experience, I have seen this repeatedly – we lead and innovate, our competitors then copy us. A computer virus called Stuxnet[46],

---

[43] The Verge, "Hackers reportedly used a tool developed by the NSA to attack Baltimore's computer systems", May 25, 2019; https://www.theverge.com/2019/5/25/18639859/baltimore-city-computer-systems-cyberattack-nsa-eternalblue-wannacry-notpetya-cybersecurity

[44] Nittany Nation, "Former govt. agent admits illegally spying on Sharyl Attkisson, implicates govt. colleagues", January 9, 2020; https://bwi.forums.rivals.com/threads/former-govt-agent-admits-illegally-spying-on-sharyl-attkisson-implicates-govt-colleagues.257893/

[45] Atlantic Council, "Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets", November 8, 2021; https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/

[46] C/NET, "Stuxnet delivered to Iranian nuclear plant on thumb drive", April 12, 2012; https://www.cnet.com/news/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/

was planted by someone into the Iranian nuclear environment, and Agent BTZ[47] was planted right back onto U.S. Government networks in a seemingly copycat attack, leveraging very similar techniques. Some may argue this as sheer coincidence, but in this gray shadow world, coincidences are often not.

43. The Chinese especially, fastidiously, laboriously, and almost to comic levels study and analyze everything, everything we say and do. If we possibly used remote access operations to enter critical infrastructure and influence events, the Chinese surely studied our efforts and applied these same capabilities and strategies. Totalitarian nations such as China, Russia, Iran, and Venezuela were always watching us, and starting with China's relentless intellectual property theft and destruction of the American economy since the 1990s and Russia's cyber aggression against Estonia in 2007, that's exactly what happened – and they have used remote access operation tactics, techniques, and procedures they often watched, studied, and learned from us.

Securing the American cyber world (and American dominance with absolute freedom of maneuver in cyber): The CNCI program established the BC/AD of remote access operations on scale

44. The CNCI effort was a grand, bold, and expensive move forward to help America re-establish dominance in the cyber arena as it was realized that threat actors were de-stabilizing and taking advantage of the American public and private information technology sectors. There were 12 publicly announced initiatives in the CNCI program[48].

---

[47] Council on Foreign Relations, "Agent.btz", November 2008, https://www.cfr.org/cyber-operations/agentbtz
[48] IT Law Wiki, "The Comprehensive National Cybersecurity Initiative (CNCI)", https://itlaw.wikia.org/wiki/Comprehensive_National_Cybersecurity_Initiative#Citation

Table 1: CNCI Projects and Lead Agencies

Project	Description
Trusted Internet Connections	Reduce and consolidate external access points with the goal of limiting points of access to the Internet for executive branch civilian agencies
Einstein 2	Deploy passive sensors across executive branch civilian systems that have the ability to scan the content of Internet packets to determine whether they contain malicious code
Einstein 3	Pursue deployment of intrusion prevention system that will allow for real-time prevention capabilities that will assess and block harmful code
Research and Development Efforts	Coordinate and redirect research and development (R&D) efforts with a focus on coordinating both classified and unclassified R&D for cybersecurity
Connecting the Centers (includes National Cyber Security Center)	Connect current cyber centers to enhance cyber situational awareness and lead to greater integration and understanding of the cyber threat
Cyber Counterintelligence Plan	Develop governmentwide cyber counterintelligence plan by improving the security of the physical and electromagnetic integrity of U.S. networks
Security of Classified Networks	Increase the security of classified networks to reduce the risk of information contained on the government's classified networks being disclosed
Expand Education	Expand education efforts by constructing a comprehensive federal cyber education and training program, with attention to offensive and defensive skills and capabilities
Leap-Ahead Technology	Define and develop enduring leap-ahead technology, strategies, and programs by investing in high-risk, high-reward research and development and by working with both private sector and international partners
Deterrence Strategies and Programs	Define and develop enduring deterrence strategies and programs that focus on reducing vulnerabilities and deter interference and attack in cyberspace
Global Supply Chain Risk Management	Develop multi-pronged approach for global supply chain risk management while seeking to better manage the federal government's global supply chain
Public and Private Partnerships "Project 12"	Define the federal role for extending cyber security into critical infrastructure domains and seek to define new mechanisms for the federal government and industry to work together to protect the nation's critical infrastructure

Figure 4: The 12 public facing "Initiatives" of CNCI

45. I was a key player in the de-classification of the 12 CNCI initiatives, which was a grueling and resource consuming bureaucratic exercise.

Figure 5: The "60 Day" Report under the Obama Administration, May 2009

46. The CNCI Program resided in the Intelligence Community (IC) under Title 50 and its budget, National Intelligence Program[49] (NIP), which is not publicly revealed except in aggregate at the end of the Fiscal Year. For the layperson, this is the world of "Black" programs. This is the budget for everything "off book", "black", or whatever other moniker is appropriate. It was my job from 2007 – 2014 to act as the senior DoD lead working in conjunction with OMB, the DNI, DHS, and the DOJ to ensure these CNCI funds were properly deployed, obligated, implemented, and effectiveness measured.

[49] Office of the Director of National Intelligence, U.S. Intelligence Community Budget; https://www.dni.gov/index.php/what-we-do/ic-budget

47. As the Obama Administration was seated after inauguration, they directed a sweeping "60 Day" review[50] of the CNCI effort. I participated in drafting the report which was well received in the Administration.[51] Again – behind the veil of the 12 announced initiatives shown above, other capabilities lurked involving big data collection, sorting, and analysis on a scale never seen—capabilities now seen as routine as with the public's addiction to Amazon and Google search. Simply put, these behind the veil programs established a historical inflexion point with an unprecedented ability to access, exfiltrate, analyze, and change information in critical infrastructure, which includes electronic election systems—on scale regardless of what it was or where it was. Our Great Power Competitors and their lackeys have once again, studied, and replicated our efforts.

48. One curious oddity of my time with CNCI and the White House was the reference to the cessation of the effort[52] to find out more about the Smartmatic Voting Machine System[53] and their curious footprint in Venezuela. At the time, it was one of many factoids/quick blurbs that came and went. In my professional viewpoint, Venezuela is acting as a foreign base camp and covert base of adventurist opportunities for China, Russia, and Iran in our home hemisphere, and it should be of significant intellectual interest as to why foreign powers are creating voting machine software in Venezuela[54]. In November 2019, I was asked to lead a cybersecurity panel on the security of Election Machines at a cyber investors event at the Washington Press Club. Jerome Lovato[55] of the Election Assistance Commission (EAC), was going to be part of the panel and he asked if Chris Wlaschin of

---

[50] Eric A. Greenwald, "History Repeats Itself: The 60-Day Cyberspace Policy Review in Context", https://jnslp.com/wp-content/uploads/2010/08/05_Greenwald.pdf
[51] Executive Office of the President, "Cyberspace Policy Review", May 2009, https://irp.fas.org/eprint/cyber-review.pdf
[52] https://www.nytimes.com/2006/10/29/washington/29ballot.html
[53] Voter Action, "SEQUOIA VOTING SYSTEMS, INC. USES VOTE-COUNTING SOFTWARE DEVELOPED, OWNED, AND LICENSED BY FOREIGN-OWNED SMARTMATIC, A COMPANY LINKED TO THE VENEZUELAN GOVERNMENT OF HUGO CHÁVEZ", June 12, 2008; https://www.nist.gov/system/files/documents/itl/vote/SequoiaSmartmaticReport61208.pdf
[54] G News, "The link Between Dominion, Sequoia, Smartmatic, and the CCP", November 21, 2020; https://gnews.org/577635/
[55] Fulcrum, "Federal slap on the wrist for a voting equipment maker's misleading claims", August 14, 2020; https://thefulcrum.us/election-security-2646984614

Election Systems & Software ("ES&S"), one of the election machines companies, could also be on the panel. It is interesting that Wlaschin, an invitee of Lovato, swiftly dismissed my proposed agenda to address Venezuela and election machine software development. Wlaschin's response shown below which included the reference to Venezuela and election machine software (Please see Figure 6 and 7 below).

Wlaschin, Chris SINET October 25, 2019 at 5:08 PM
RE: REMINDER: SINET Showcase WDC Panel Prep Call (Panel 10)
To: [redacted] & 4 more Details

Janice, thank you for setting this up and providing an abstract. I think this panel will be able to develop more timely and relevant questions than those proposed and I would ask our panel members to do just that. 2006 and 2016 are far behind us and we have plenty to talk about regarding recent challenges and opportunities.
Chris

-----Original Appointment-----
From: [redacted]>
Sent: Friday, October 25, 2019 2:41 PM
To: John Mills; Wlaschin, Chris;[redacted]v; Jerome Lovato
C[redacted](CTR)
Subject: REMINDER: SINET Showcase WDC Panel Prep Call (Panel 10)
When: Monday, October 28, 2019 1:30 PM-2:00 PM (UTC-08:00) Pacific Time (US & Canada).
Where: United States: +1 712 451 0200, Access code: 181363

Hello -
THANK YOU for your upcoming participation at SINET Showcase in Washington DC.

Our panel prep call to discuss the upcoming panel:
Monday, October 28th @ 4:30pm ET / 3:30 CT / 1:30pm PT (if this time does not work, please let me know)
Dial-in using your phone:
United States: +1 712 451 0200
Access code: 181363
Please find the panel abstract attached.

Event Site: https://www.security-innovation.org/events/dc/
You are currently on our agenda on the following panel:
Wednesday, November 6, 2019
4:50 PM – 5:30 PM
What Are We Doing To Improve Election Security and Interference?

Figure 6: Email Exchange where Mr. Wlaschin dismisses my proposed agenda points referencing Venezuela and Election Machine software development.

structure today is over seen by local jurisdictions and conducted mostly by volunteers. It was not designed or created in the context of delivering voting resilience in the face of determined adversaries – but that is the reality today. This panel will discuss some of the challenges – but also some of the reasonable ways ahead to provide higher levels of assurance and confidence in the voting system.

Scope and Scale of US Elections

Roughly 114,000 Polling Stations nationwide

Roughly 174,000 Precincts

Roughly 350,000 voting "machines" in the system

Precinct size is roughly 1,100 voters

Low end is roughly 437 in Kansas/2,704 in DC

Potential Questions:

Who here has helped run an election (been an "election official") in the US and/or overseas?

How can technology make things better?

A NYT October 29, 2006 article talked about a US investigation into Smartmatic/Sequoia and Venezuela – what ever happened to that?

Is diversity of voting machines and processes helpful or a vulnerability?

Would standardizing methodologies across all 174k precincts help or make things worse?

Figure 7: Agenda Attachment to Email Exchange where Mr. Wlaschin dismisses my proposed agenda points referencing Venezuela and Election Machine software development.

49. During my government service I witnessed the development of a close relationship between the Obama / Biden Administrations, the Federal Government and Big Tech in Silicon Valley. The beginnings of this relationship can be traced in part to the 2006 – 2007 timeframe when the Commander of a Combatant Command had his Facebook site hacked. At the time, the Department of Defense didn't really have firm policy on social media usage or protection of the public personae of senior personnel. I was called in and told by the senior, Senate Confirmed Assistant Secretary of Defense to figure it out and give control of the account back to the Combatant Commander. I simply picked up the phone and after a few calls was talking to former DOJ prosecutor, then Facebook Chief

Security Officer Joe Sullivan[56]. With no formal process or memorandum of agreement in place, within the day, the Commander had his Facebook account back. Establishing and formalizing the Silicon Valley and DOD/U.S. Government relationship became one of my core missions from 2009 to 2016 in addition to CNCI, and it has now been memorialized as the DIU[57].

Office of Personnel Management – a massive Chinese remote access operation with horrific and real results

50. While significant people, programs, and resources were being generated by CNCI, the Chinese conducted a massive remote access penetration and exfiltration operation focused on the obscure, and not well known, Office of Personnel Management ("OPM"). This was a brilliant flanking action by Chinese intelligence to "vacuum up" massive amounts of information and illustrates how American critical infrastructure involving electronic systems can be penetrated through remote access operations. The more recent Solar Winds breach is one more example of a nation state using remote access operations to penetrate a critical infrastructure network (including U.S. Government Departments and Agencies) and planting enabling malware (one may also say algorithms) to enable further distribution of the malware and embedding the malware/algorithm into updates which created broad and pervasive presence through many customer networks using Solar Winds Orion software. This was one more example of the relative ease of the offense penetrating the defense and spreading broadly, perhaps for years, and establishing a decisive position to monitor, surveil, steal, and manipulate data[58]. This breach also illustrates how thousands of systems can be hacked in a coordinated fashion, and shows how the

---

[56] Wired, "A Former Uber Exec's Indictment is a Warning Shot", August 21, 2020; https://www.wired.com/story/uber-exec-joe-sullivan-data-breach-indictment/
[57] Defense Innovation Unit; diu.mil
[58] Trenton System, "SolarWinds Orion Hack Explained", https://www.trentonsystems.com/blog/solarwinds-hack-overview-prevention

belief that our electronic voting systems are more secure by being purportedly decentralized is a false notion

51. The decisive way China conducted the OPM breach demonstrated the ease at which a peer competitor could access a U.S. Government "trusted" critical infrastructure network, install enabling malware, and exfiltrate data on a massive scale. The crown jewel of this massive theft through remote access[59] were the hundreds of thousands or more SF-86's[60]—the key U.S. Government form that comprehensively documents all of the information about a person's history and background for those seeking or renewing a security clearance that were taken. CNN reported 21.5 million Americans were exposed in this breach[61] which started, perhaps around 2013, just as CNCI was hitting full operational capability. These files contained expansive details about everyone who has or had security clearances. The FBI has made some arrests – one Chinese personality was so brazen as to be traveling in the U.S. at the time of his arrest[62], however the loss has been catastrophic.

52. According to one report – the CIA's agent network was destroyed in China[63] and the Chinese aggressively used the information derived in the breach for spying operations[64]. It is very likely Chinese nationals were arrested and dispensed with from this historic, catastrophic security breach. I lived through the response actions inside the Government. This episode must be highlighted as an

---

[59]CSO, "The OPM hack explained: Bad security practices meet China's Captain America
How the OPM hack happened, the technical details, and a timeline of the infiltration and response." February 12, 2020 https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

[60] Big data analytics can consume this information and cross reference, analyze and find interesting connections and lack of connections that can be ques for intelligence analysis. https://www.opm.gov/forms/pdf_fill/sf86-non508.pdf

[61] CNN, OPM Data Breach, July 9, 2015, https://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/index.html

[62] The Hill, FBI arrests Chinese national linked to OPM Hack Malware, https://thehill.com/policy/cybersecurity/347897-fbi-arrests-chinese-national-linked-to-opm-hack-malware-report

[63] CNN, "U.S. pulls spied from China after hack", https://money.cnn.com/2015/09/30/technology/china-opm-hack-us-spies/

[64] Schneier on Security, December 24, 2020, https://www.schneier.com/blog/archives/2020/12/how-china-uses-stolen-us-personnel-data.html

example showing the scope and effects of remote access operations. There is no reason to believe that our electronic election systems infrastructure could not be similarly penetrated and manipulated.

The Cyber Response Group (CRG) handles the hardest Cyber Problem Sets

53. From about 2008 – 2014, I was one of a small group of inter-agency players involved in a group called the CRG. The purpose of this group was to work the hardest problem set of weaknesses of the American cyber critical infrastructure to foreign remote access operations and turn these into opportunities for American counter moves back into the threat environment to hold our adversaries at risk. The name morphed over time and the small, inter-agency group appreciated my unique and actionable insights. In approximately 2014, because of shifting priorities, I no longer attended the CRG meetings, but I often heard updates of their work in in regular internal cyber coordination meetings. Usually, it was the representatives from Undersecretary of Defense for Policy, starting with Eric Rosenbach who would share these hints. In 2016, references to Russian and Chinese interference into the American election process began. The references identified their intrusions into campaign networks. Iran was also a regular threat nation identified.

54. At other times, I observed references being made by senior officials on the clever use of information FVEYES partners provided to spy on Americans. These FVEYES techniques were long standing and pre-existing as a possibly lawful end-around the FISA process, but rarely used. The unlawful un-masking operation against Trump Campaign personnel, revealed later, caused me to believe that the CRG Group was possibly the group and entry portal for compartmented activity to support spying on the Trump Candidacy and nominate names for un-masking. Several days after the election in November 2016, I was called by a group member on the classified phone and asked to participate in the production of the ICA to finalize the Russian Narrative with Trump as a Russian asset with the purpose of delaying the January 2017 inauguration of President Trump. Now we know

through the de-classifications by Mr. Richard Grennell and Mr. John Ratcliffe, that Comey and Brennan knew the Russia Story was false, but they personally pushed through an ICA (which I non-concurred with during my assigned review, due to the lack of substantiating detail) in late November 2016 to January 2017 to frame President Trump and potentially block his inauguration.

Failure of the U.S. Government to Secure the American Election Environment

54. One point of concern that is relevant are the assertions by U.S. Government Officials on the security of U.S. election critical infrastructure against remote access operations. Election security was a topic raised several times while I was in office. As I become knowledgeable of the election process in the United States, since leaving office, and knowing a fair amount about the maturity, ability, operations, and true, overall priorities of the different U.S. Government Cybersecurity Centers such as CISA, the NSA Threat Operations Center (NTOC), the FBI National Cyber Investigative Joint Task Force (NCIJTF)[65], and other U.S. Government entities, while the leaders and personnel are of high caliber and well meaning, they simply do not understand the election system, process, nor equipment.

55. Around the November 2020 election, representatives of CISA, including Mr. Chris Krebs, Director of CISA, made strong assertions of election security such as "[t]he November 3rd election was the most secure in American history." In my professional opinion, such statements are false because, in my observations and decades of experience within government, the U.S. Government does not have the people, programs, or resources to have a comment on the true resilience and security of the election critical infrastructure.

---

[65] FBI, NCIJTF, https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force

56. In addition, two things Mr. Krebs did, significantly undermined his credibility. First was his tweet on November 18, 2020, where Mr. Krebs backtracked on his previous assertion of that the November 2020 election was secure.

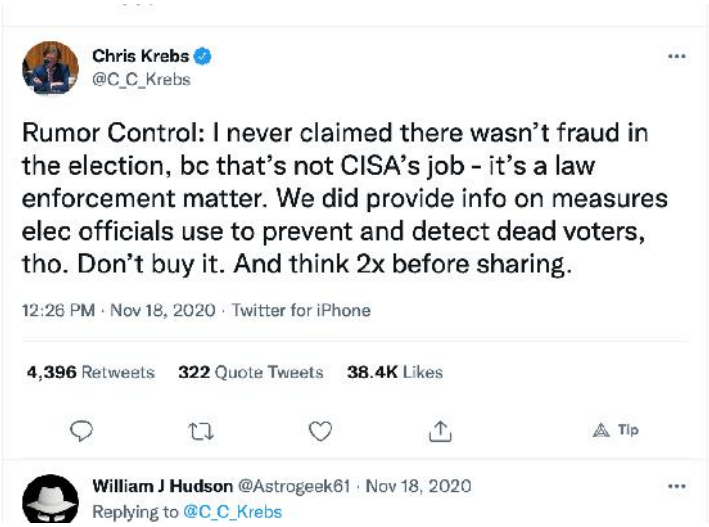


Figure 6: Mr. Chris Krebs Tweet on November 18, 2020

57. The second was Mr. Krebs congressional testimony on February 10, 2021[66], where his statement was replete with comments on the shortage of people, programs, or resources to provide effective cybersecurity of the American election environment. From Mr. Krebs statement, it is hard to reconcile his February 10, 2021, statement with the statement he approved from November 12, 2021:

> "It is hard to overstate the massive scope of the critical infrastructure security and resilience challenge. The levers government has at its disposal to change behaviors, on the other hand, is underwhelmingly small.

[66] Christopher C. Krebs Testimony before Committee on Homeland Security, February 10, 2021, https://docs.house.gov/meetings/HM/HM00/20210210/111152/HHRG-117-HM00-Wstate-KrebsC-20210210.pdf

This leads to three conditions limiting the ability of government and industry to collectively improve critical infrastructure cybersecurity: (1) lack of a deep understanding of what is truly systemically important across the economy, (2) a need for more meaningful methods for operational engagement with industry to address risk; and (3) insufficient funding and investment in security improvements. "

58. Knowing these things, and the maturity of CISA, in my professional opinion, Mr. Chris Krebs was in over his head with attempting to lead a U.S. Government agency. He should have been more transparent on the state of affairs, yet if he did, it likely would have revealed a political appointee unable to exercise effective leadership of an organization.

59. In my professional experience and opinion, it is of low probability that the national intelligence collection system was specifically looking for Chinese intervention into any election system infrastructure or components. The catastrophic Target Corporation (The Target retail store) breach[67] demonstrated how a threat actor can remotely obtain access into key information of an enterprise through related but different critical infrastructure such as facility climate control networks (i.e., HVAC Heating, Ventilation, Air Conditioning). The Target Corporation breach was closely followed and studied within the U.S. Government. It is of note that none other than Chris Krebs identified this capability of remote access through a related system in a 2014 article on the Target Breach[68].

In my professional opinion, assertions by state and federal officials that electronic election systems in our Country are secure from remote access operations have little basis in fact and are false. My

---

[67] ZDNet, "The Target Breech, two years later", November 27, 2015, https://www.zdnet.com/article/the-target-breach-two-years-later/

[68] KrebsonSecurity, Target hackers Broke in via HVAC Company, February 14, 2015, https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

opinion is further supported by other computer science experts such as University of Michigan Professor J. Alex Halderman.[69]

I declare under penalty of the perjury laws of the State of Virginia and the United Sates that the foregoing is true and correct and that this declaration was executed this 21st day of November 2021 in Woodbridge, Virginia

Colonel, USAR (Retired) John R. Mills
November 21, 2021

[69] Declaration of J. Alex Halderman in support of Motion for Preliminary Injunction, Civil Action No. 1:17-CV-2989-AT stating 16 states using Dominion machines can have votes "stolen" by "nefarious actors" and begging the court unseal his report on these issues to allow CISA to try and fix these vulnerabilities before the 2022 election.

EXHIBIT 5

Declaration of J. Alex Halderman (Sept. 21, 2021)

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**DECLARATION OF** **J. ALEX HALDERMAN** **Civil Action No. 1:17-CV-2989-AT**

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2. My July 1, 2021, expert report describes numerous security vulnerabilities in Georgia's Dominion ICX BMDs. These include flaws that would allow attackers to install malicious software on the ICX, either with temporary physical access (such as that of voters in the polling place) or remotely from election management systems. They are not general weaknesses or theoretical problems, but

rather specific flaws in the ICX software, and I am prepared to demonstrate proof-of-concept malware that can exploit them to steal votes cast on ICX devices.

3. Some of these critical vulnerabilities could be at least partially mitigated through changes to the ICX software if Dominion implemented such changes and jurisdictions deployed them. However, it would likely take months for Dominion to assess the problems, develop responsive software updates, test them, obtain any necessary approvals from the EAC and state-level certification authorities, and distribute the new software to states, as well as additional time for localities to install the changes. But Dominion cannot begin this process, because (to my knowledge) they have yet to learn what is in my report.

4. My analysis also concludes that the ICX is very likely to contain other, equally critical flaws that are yet to be discovered. Jurisdictions can mitigate this serious risk through procedural changes, such as reserving BMDs for voters who need or request them. Election officials cannot make an informed decision about such urgent policy changes or any other mitigations until they have assessed the technical findings in my report. However, to my knowledge, the Georgia Secretary of State's Office has yet to even request access to it, despite Plaintiffs' repeated offers to make it available to appropriate individuals at the Secretary's Office.

5. Nor do these problems affect Georgia alone. In 2022, the ICX will be used in parts of 16 states.[1] Nevada will use it as the primary method of in-person voting in certain areas of the state. Louisiana is slated to use it for early voting in a DRE configuration where there is not even a paper trail. It will be used for accessible voting in Alaska and large parts of Arizona, California, Colorado, and Michigan. It will also see some use in parts of Illinois, Kansas, Ohio, Missouri, New Jersey, Pennsylvania, Tennessee, and Washington State. Officials in these jurisdictions too must act to update the software and their procedures, but they cannot do so without information about the problems. Continuing to conceal those problems from those who can—and are authorized to—address them, to the extent possible, serves no one and only hurts voters (and heightens the risk of compromise in future elections).

6. The most effective way to ensure that the necessary information gets to the parties responsible (without also falling into the wrong hands) would be to share my report with the Cybersecurity and Infrastructure Security Agency (CISA), which operates a Coordinated Vulnerability Disclosure (CVD) program for just this purpose. CISA is a federal agency that collaborates with state and local governments, election officials, federal partners, and vendors to manage risks to U.S. election

---

[1] See Verified Voting, "Verifier Search – November 2022," https://verifiedvoting.org/verifier/#mode/search/year/2022/model/ImageCast%20X.

infrastructure.[2] Under CISA's CVD process, agency staff would independently validate the vulnerabilities, work with Dominion to develop software updates as necessary, and facilitate sufficient time for affected states and localities to apply mitigation strategies.[3] CISA strives to disclose "accurate, neutral, objective information focused on technical remediation and mitigation" and to "correct misinformation where necessary,"[4] making it well qualified to coordinate the disclosure of such sensitive vulnerabilities.

7. Geoff Hale, Director of CISA's Election Security Initiative, has confirmed to me that, if the Court permits it, the agency would be willing to receive my expert report and carry out coordinated vulnerability disclosure activities as appropriate (see Exhibit 1). Mr. Hale requests that I and my assistant Drew Springall be available for consultation with CISA during the CVD process, which we would be willing to do subject to the Court's permission.

8. Informing responsible parties about the ICX's vulnerabilities is becoming more urgent by the day. Foreign or domestic adversaries who are intent on

---

[2] Cybersecurity and Infrastructure Security Agency, "Election Infrastructure Initiative," https://www.cisa.gov/election-security.
[3] Cybersecurity and Infrastructure Security Agency, "Coordinated Vulnerability Disclosure Process," https://www.cisa.gov/coordinated-vulnerability-disclosure-process.
[4] *Id.*

attacking elections certainly could have already discovered the same problems I did, yet Georgia's 2022 primaries are less than nine months away, and other states that use the ICX will conduct high-profile elections even sooner. It is important to recognize the possibility that nefarious actors already have discovered the same problems I detail in my report and are preparing to exploit them in future elections. Providing my report to CISA through its CVD program will ensure that Dominion and affected jurisdictions are able to begin appropriate mitigations as soon as possible. Continuing to withhold my report from CISA puts voters and election outcomes in numerous states at unnecessary, and avoidable, risk.

9. I understand that State Defendants object to disclosure to CISA on the argument that my report should be used only for this lawsuit. But this ignores the implications of my report and my role in this matter. I am not a party to this lawsuit. I am an independent expert who was engaged to conduct an impartial assessment of the security and reliability of the Dominion BMD system, using (in part) election equipment that the Court ordered I be provided. I have done that, as reflected in my lengthy, detailed report and other submissions in this matter. As an independent expert and member of the election integrity community, I have a professional obligation to take appropriate steps to ensure that the severe vulnerabilities my report describes are properly remediated, to the extent possible, and that those tasked with

election security and administration across the country have the information they need to make responsible, informed decisions about election procedures, including the equipment used, the manner and purposes for which it is used (including whether it is used at all), the steps needed to secure that equipment and other aspects of the election systems in which it is used, and more. In short, my professional obligations do not end at the boundaries of this lawsuit, nor do the serious risks to voters and elections that my report discusses in depth. Additionally, I can imagine no prejudice to anyone in this lawsuit (or beyond) from disclosure of my report to CISA, nor am I aware of any claim of prejudice from any of the parties.

10. I of course have complied, and will continue to comply, with all directives from the Court regarding disclosure of my work in this matter. I submit this declaration to explain why I believe disclosure of my report to CISA is critically important (and not just for Georgia) and to respectfully ask that the Court allow that disclosure, rather than accept State Defendants' position that my findings must not be shared beyond the confines of this lawsuit, including with those who are authorized to address the vulnerabilities with the ICX and stand ready to do so. If my findings regarding the ICX actually present no meaningful risks to voters and election outcomes and therefore require no remediation, as I gather State Defendants would have the Court believe, CISA is well positioned to determine that. If, on the other

hand, my findings do warrant remediation, as I believe they do, then CISA is well positioned to work with Dominion and the appropriate authorities around the country to implement remedial measures. I can see no reason to prevent (or further delay) that important work for future elections. And I note that none of State Defendants' experts have disputed my findings regarding the ICX machines. Only Dr. Juan Gilbert has responded to my sealed report, and he has not examined the machines (or used them) to my knowledge.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 21st day of September, 2021 in Ann Arbor, Michigan.

J. ALEX HALDERMAN

Gmail

J. Alex Halderman <halderman@gmail.com>

Vulnerability Disclosure

Hale, Geoffrey <Geoffrey.Hale@cisa.dhs.gov> Thu, Aug 19, 2021 at 12:15 PM
To: "J. Alex Halderman" <jhalderm@umich.edu>
Cc: Andrew Springall <andrew.springall@gmail.com>

Prof. Halderman,

Thank you for your email. Yes, CISA would be willing to receive the report regarding possible vulnerabilities in election infrastructure for inclusion in CISA's Coordinated Vulnerability Disclosure (CVD) process and would carry out any further coordinated disclosures activities as appropriate. As we share on our public website (https://www.cisa.gov/coordinated-vulnerability-disclosure-process), CISA's CVD program coordinates the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services with the affected vendor(s). Note that part of our process may also involve validating any alleged vulnerabilities, planned mitigations, remediations, or patches with the security researcher who discovered the alleged vulnerability, so we would appreciate if you could continue to be available for consultation during the CVD process as well.

As shared on our website, please submit any vulnerability reports for CVD coordination using the form here: https://www.kb.cert.org/vuls/report/

Best,

Geoff

From: J. Alex Halderman <jhalderm@umich.edu>
Sent: Wednesday, August 18, 2021 4:37 PM
To: Hale, Geoffrey <Geoffrey.Hale@cisa.dhs.gov>
Cc: Andrew Springall <andrew.springall@gmail.com>
Subject: Vulnerability Disclosure

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Dear Mr. Hale,

We are writing to you in your capacity as Director of the Election Security Initiative at the federal Cybersecurity and Infrastructure Security Agency (CISA).

We understand that the Election Security Initiative at CISA works to ensure the physical security and cybersecurity of the systems and assets that support the Nation's elections, including through detection and prevention, information sharing and awareness, and incident response.

As you may be aware from recent press reports, one of us (Halderman) is presently serving as an expert witness for the plaintiffs in Curling v. Raffensperger (Civil action no. 1:17-CV-2989-AT, N.D. Ga.), a case that concerns the security of Georgia's election system. A year ago, the court granted plaintiffs access to an ICP ballot scanner and ICX ballot marking device as used in Georgia in order to test their security. Following months of analysis, on July 1, Dr. Halderman submitted an expert report that describes several very serious vulnerabilities we found in the equipment, which, to our knowledge, have not been previously documented or disclosed.

Given the nature of the vulnerabilities and the time that would be necessary to mitigate them before the 2022 midterm elections, we believe it is critical for Dominion and affected jurisdictions (which include Georgia and parts of many other states) to begin taking responsive action soon. It is also vitally important to prevent information sufficient to exploit the vulnerabilities from falling into the wrong hands, and to avoid fueling election-related misinformation if possible.

Currently, disclosure of the expert report to anyone other than outside litigation counsel for the parties is strictly prohibited by the Court’s protective order and by recent directives from the judge. However, if permitted by the Court, we would like to share the report with CISA and ask your agency to carry out appropriate further disclosure of the information it contains to Dominion and affected jurisdictions as you see fit, under CISA's coordinated vulnerability disclosure (CVD) program (https://www.cisa.gov/coordinated-vulnerability-disclosure-process).

We understand that under this process, CISA will work with the vendor (Dominion) for mitigation development and the issuance of patches or updates and to facilitate sufficient time for affected end users to obtain, test, and apply mitigation strategies. We further understand that CISA strives to disclose "accurate, neutral, objective information focused on technical remediation and mitigation" and to "correct misinformation where necessary".

Please confirm that CISA would be an appropriate agency to handle coordinated vulnerability disclosure for election infrastructure under these circumstances, and that you would be willing to receive the report (subject to the Court's permission) and carry out further disclosures as you deem appropriate.

Sincerely,

J. Alex Halderman

Drew Springall

EXHIBIT 6

Email, Steven Rosenberg, Fulton County Deputy County Attorney to Garland Favorito (Sept. 27, 2021)

GARLANDF@msn.com

From: Rosenberg, Steven <Steven.Rosenberg@fultoncountyga.gov>
Sent: Monday, September 27, 2021 9:57 AM
To: GARLAND FAVORITO
Cc: Bodison, Mariska; Ringer, Cheryl; Lowman, David; McCray, Unique; Eatmon, Shana
Subject: RE: VoterGA Open Records Request #1 - 09-27-21

Mr. Favorito,

I recall our conversation and I appreciate you emailing me your requests. I can confirm that the County maintains no records which are responsive to your request. The answer is the same for both the request contained in this email as well as the email you just sent seeking "*Electronic Copy of the approximately 315,000 original In-Person Advance Voting ballot images for the November 3rd, 2020 election*". The County maintains nothing responsive.

Steve Rosenberg
Deputy County Attorney
Office of the County Attorney
404-612-0259(direct)
404-612-0246 (main)
404-730-6324 (fax)
Connect with Fulton County:
Website | Facebook | Twitter | Instagram | FGTV | #OneFulton E-News

This message (including any attachments) is being sent by or on behalf of a lawyer. It constitutes an electronic communication within the meaning of the Electronic Communications Privacy Act, 18 U.S.C. §2510, and its disclosure is strictly and exclusively intended for the individual or entity to which it is addressed. This message may contain information that is protected by the attorney-client privilege and/or the attorney work product doctrine, and may be proprietary, privileged, confidential, or otherwise legally exempt from disclosure. If you are not a named addressee, you are not authorized to read, use, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail, and please delete from all locations all copies of the message without reading or saving any part in any manner.

From: GARLAND FAVORITO [mailto:GARLANDF@msn.com]
Sent: Monday, September 27, 2021 9:38 AM
To: Rosenberg, Steven <Steven.Rosenberg@fultoncountyga.gov>
Cc: Bodison, Mariska <Mariska.Bodison@fultoncountyga.gov>
Subject: VoterGA Open Records Request #1 - 09-27-21

Attorney Rosenberg,
Prior to the hearing last week, I mentioned that I had two more Open Records requests and I believe you said you preferred me to Email them to you. I understand that Fulton Elections may not have this information and if so, a simple confirmation that there are no responsive records is all that is needed. The request is:

- *"Electronic Copy of all original Election Day ballot images for the November 3rd, 2020 election"*

I have one additional request I will send in a separate Email. I am copying Ms. Bodison since I know she will be working with you to respond to these requests.

Thank you,

Garland Favorito
VOTERGA.ORG
404 664-4044 CL

EXHIBIT 7

Email, Chris Harvey, Georgia Election Director, to Larry Sampson, Murray Cty., Georgia (Dec. 2, 2020)

Larry Sampson

From: Chris Harvey <wchrisharvey@gmail.com>
Sent: Wednesday, December 2, 2020 1:12 PM
To: Larry Sampson
Subject: Re: memory cards

Yes, go ahead and reuse the memory cards.

On Tue, Dec 1, 2020 at 09:59 Larry Sampson <lsampson@murraycountyga.gov> wrote:

> Hello Chris: We really need to know if it is ok to clean the memory cards we used in the scanners in the General Election or do they need to stay loaded for some legal reason. It is time to start L&A and Dominion sent no extra cards with the equipment,
>
> Larry
>
> Murray

--
Chris Harvey

EXHIBIT 8

Sen. William Ligon, Chairman, Election Law Study Subcommittee of the Georgia Standing Senate Judiciary Committee (Dec. 17, 2020)

REPORT

OF THE ELECTION LAW STUDY SUBCOMMITTEE OF THE STANDING SENATE JUDICIARY COMMITTEE

SUMMARY OF TESTIMONY FROM DECEMBER 3, 2020 HEARING

Honorable William T. Ligon, Chairman
Senator, District 3

_____

Honorable John Kennedy, Member
Senator, District 18

_____

Honorable Bill Heath, Member
Senator, District 31

_____

Honorable Blake Tillery, Member
Senator, District 19

_____

Honorable Michael Rhett, Member
Senator, District 33

_____

Honorable Elena Parent, Member
Senator, District 42

_____

I. INTRODUCTION

II. EXECUTIVE SUMMARY

III. ORAL TESTIMONY

IV. FINDINGS

V. RECOMMENDATIONS

I. INTRODUCTION

The charge assigned to the Election Law Study Subcommittee of the Standing Senate Judiciary Committee was to examine the recent election cycle, the recount process, the audit process, the current investigations taking place, the litigation that is moving forward, as well as address issues relating to the upcoming runoffs. In the matter of the law itself, we were to also consider Georgia's election laws as they have impacted and are impacting the current election cycle. This Report may be further amended prior to the 2021 Georgia Legislative Session.

This Subcommittee met once at the Georgia State Capitol on Thursday, December 3, 2020. The hearing was open to the public, and there was an open invitation for citizens to speak before the committee. Subcommittee members also expressed stories they had heard from their constituents. Other committee meetings have also been hearing testimony which should be considered to present an even broader understanding. At this time, the additional committees which have met and received testimony are the Senate Governmental Affairs Committee and the House Governmental Oversight Committee. Many who could not testify due to lack of time have recorded their own testimonies online and shared their written speeches with this committee; the Subcommittee received many affidavits under oath.

II. EXECUTIVE SUMMARY

The November 3, 2020 General Election (the "Election") was chaotic and any reported results must be viewed as untrustworthy. The Subcommittee took evidence from witnesses and received affidavits sworn under oath. The Subcommittee heard evidence that proper protocols were not used to ensure chain of custody of the ballots throughout the Election, after the opening of ballots prior to the Election, and during the recounts. The Subcommittee heard testimony that it was possible or even likely that large numbers of fraudulent ballots were introduced into the pool of ballots that were counted as voted; there is no way of tracing the ballots after they have been separated from the point of origin. The Subcommittee heard testimony of pristine ballots whose origin looked suspicious or which could not be verified and the inability of poll workers to distinguish between test ballots and absentee ballots. Signatures were not consistently verified according to law in the absentee balloting process.

Poll watchers on Election Night testified that they had noted that ballots were not secured, that seals and security tags were not used, and the chain of custody was often lax or non-existent. During the recount process, the monitors observed similar patterns of unsecured ballots that had broken seals and open cases of ballots laying around for hours or overnight in unsecured locations. There was a lack of enforcement of the law, sloppy handling of the ballots by those counting, deliberate covering-up of voting numbers by workers, lack of following the process during the recount, unsafe handling of military ballots, and insecure data such as on laptops and flash drives. According to submitted testimony, there were also many equipment failures when ballots would not go through the machines and other times when ballots were counted more than once.

A great deal of testimony supported evidence of a coordinated effort to prevent a transparent process of observing the counting of ballots during the absentee ballot opening period and on Election Night. Witnesses testified to hostility to Republican poll workers during the recount – directional signage was unavailable, doors were locked, and Republican poll watchers were sent home early or given menial assignments.

Monitors throughout the state were often kept at an unreasonably long distance – some social distancing was understandable, but monitors were blocked from having the visual ability to see what was written on the ballots or to have any meaningful way to check the counting or to double-check that what was counted was actually assigned to the right candidate. They also could not observe what was entered into the ARLO system, nor could they be told the count that was being entered into ARLO. Instead, they were told that those numbers would be totaled and come back from the Secretary of State's Office. They were also told not to take pictures, film, or have other means of acquiring proof of the process that they were experiencing based on a rule from the State Elections Board. That rule contravenes the spirit and purpose of the election law.

The Secretary of State's Office was unresponsive to its hotline. It has been unresponsive to many who wonder if their vote ever really counted. The office has turned a blind eye to fraud to the point that it ought to be considered gross negligence.

The Subcommittee did not have time to investigate the numerous publicly reported issues with the Dominion voting machines. The Subcommittee takes notice of the various publicly reported functions of the machines and heard evidence that the machines can duplicate fraudulent ballots to the point that not even trained personnel can tell the difference between a test ballot and a real ballot. Testimony also suggested that the system responds wirelessly to being reset from an unknown location as happened with the poll books. The Subcommittee also heard that Dominion machines can be programmed with algorithms that reallocate votes between candidates. In addition, the Dominion machines are programmed to count votes using percentages of whole numbers rather than actual votes, which is a feature incompatible with the actual voting process. The Subcommittee learned that the history and control of the

company that owns the Dominion voting system is unclear and provides serious implications of foreign interference in the U.S. election.

III. ORAL TESTIMONY

Violation of Ballot/Computer Security Procedures During Early Voting and on Election Day

- Bridget Thorne, who has nine years' experience as a poll worker/precinct manager in Fulton County, worked for five and a half days during early voting as a technician in the temporary warehouse in the Georgia World Congress Center. Because of positive COVID tests among Fulton County elections employees, Dominion Software was selected to run the warehouse. Thorne was disturbed at the lack of ballot security. Test ballots were printed on the same type of paper (official Rolland Voting paper) as real ballots, but test ballots were not routinely marked as such or destroyed. Thorne testified she saw a stack of these ballots almost eight inches tall.

  On October 30, when early voting finished at State Farm Arena in Fulton County (the "State Farm Arena"), Thorne observed 40-50 scanners being brought into the arena and tens of thousands of ballots being scanned in by random people pulling ballots from random places – no formal procedure, no oaths, no chain of custody. When Thorne objected to this haphazard process, a Dominion employee replied, "It's fine, we have been doing this all week." When Thorne left that night, she observed unsecured suitcases of ballots next to the scanners.

  Upon arriving at the State Farm Arena the following morning, Thorne saw that suitcases of ballots had been piled in a corner and sealed. But there was no restricted access, so anyone could have removed one or more suitcases. In addition, anyone could have opened them and resealed them" because "seals were easily accessible." During the day, employees brought Thorne other ballots that were found in the warehouse, asking if they were real or test. She had no way of knowing.

  The following night, when Thorne was again working at the warehouse, she observed a Dominion employee and an Election Group Consultant printing "test ballots" but doing so incorrectly. She realized then that "anyone in the warehouse had access to printing real ballots."

  Before Election Day, Thorne attempted to report her concerns about these insecure ballot operations to the Secretary of State (SOS) office and to the State Board of Elections; she received no response.

  Since giving her testimony to the Senate Subcommittee, Bridget Thorne has been fired by a consultant working for Fulton County.

Recount: Counting Votes Without Monitoring, or Without Meaningful Monitoring

- Election Day – Video from State Farm Arena in Fulton County showed a Fulton County Election worker approaching the media and poll monitors. After a brief exchange, the media and monitors packed up and left. This coincided with media reports that everyone was told to leave State Farm Arena around 10 p.m. on Election Night; workers testified they were told that tabulation was stopping for the night and would resume the next morning. Instead, video from State Farm Arena revealed that about six workers stayed behind. What happened next revealed a coordinated effort by election workers to deliberately conceal their continued counting of ballots out of public view, in direct violation of the law. This incident was premeditated. Those workers pulled out four concealed cases of ballots from under a table and continued counting for another two hours. During those two hours there were multiple machines running, each of which could process up to 3000 ballots per hour. A "representative" of The Secretary of State's office claimed that it had a representative present during that period, and the media reported that statement widely; it was not true. The representative admitted he was not present during that time period and is not evident on the video.

- David Cross, though unable to speak at the hearing due to time constraints, submitted written testimony with graphs, one of which appears to enhance the significance of what took place with the change in vote totals just after the late-night activities took place at State Farm Arena. Due to its significance to the State Farm Arena video seen by the committee, his graph is included with this Report. It shows that 136,155 votes suddenly appeared in Biden's vote column at 1:59 a.m., November 4, 2020.

- Scott Hall of Fulton County is an experienced poll watcher who testified that there was a secured "lunch area" but when he bought lunch for workers, they were not permitted to use that area. There were no cameras in that area, yet tables were set up for counting, and poll watchers were excluded. He has photographs of the area. He also testified that there were stacks and stacks of unsecured blank ballots ("checks," as he called them) that were in the open.

- Mr. Hall noted a limitation of one monitor per 10 recounting tables as being an inadequate ratio to be truly effective. He was constantly engaged in the recount, even being called to go to the World Congress Center at ridiculous hours, such as 10 p.m., for more counting. He was adamant that something was seriously wrong with how Fulton County was handling the ballots.

- Mark Amick reported that in DeKalb County, only one monitor was allowed per 10 tables of 16 recounters. He testified that monitors were kept six feet away and could not see the totals entered on the computer screens.

- At State Farm Arena at the end of the recount day on November 14, Susan Voyles of Sandy Springs observed pallets of ballots remaining to be counted beginning the following day. When she arrived the next morning, November 15, those pallets were gone.

- On November 15, Voyles and her partner with whom she had traveled to State Farm Arena (also identified as a Republican), were given only 60 ballots to review, even though other tables had thousands. Voyles and her partner, as well as other Republican monitors, were told at 10 a.m. there was nothing else for them to do, so they should leave. Since giving her testimony to the Senate Subcommittee, Susan Voyles has been fired by a consultant working for Fulton County.

- Tony Burrison of Savannah and a military veteran served as one of very few recount observers during the recount in Chatham County. He described the process as "disgusting" – stacks of ballots were being counted with no oversight or accountability. Based on what he observed, he believed there is a major problem with voting integrity due to tampering with the vote.

- Nancy Kain of DeKalb reported that she was kept too far from the counting to verify any votes.

- Hal Soucie of Smyrna, a poll watcher at State Farm Arena, testified that he was told that he was not supposed to be close enough to see batch numbers.

No Chain of Custody

- Annette Davis Jackson, a Gwinnett monitor, saw broken locks on the bins containing paper backup ballots.

- Scott Hall of Fulton County was told to leave the World Congress Center after he tried to document and photograph nine unsecured bags of ballots. He testified he "cried" over the incidents he saw.

- Dana Smith, a Republican poll watcher in Hart County, testified that she observed the paper backup ballots being placed in unlocked canvas bags for transport to the county office of the Elections Supervisor. The precinct manager finally (at Smith's insistence) obtained locks before transporting the bags in her car, but she refused to complete chain-of-custody forms. Smith also testified that there was open access to the special paper used to print the paper backup ballots.

- Hal Soucie observed the recount process in two counties, Cobb and Fulton. At State Farm Arena in Fulton County, he reported "suitcases" full of ballots "all over the place," with no chain-of-custody procedures, no time and no date information. He observed people taking ballots out of the cases, counting, and putting them right back into the cases. No one checked him in as a credentialed observer, and one man handed him a stack of ballots without knowing who he was or where the ballots came from.

Suspicious "Pristine" Absentee Ballots

- At the State Farm Arena recount on November 14, Susan Voyles – who has 20 years' experience managing election precincts in Fulton County – reviewed a stack of 110 absentee ballots [ballots are normally placed in stacks of 100] and noticed they were "pristine." They had not been folded, and they did not appear worn as though voters and election workers had handled them. Each ballot was "bubbled in" with exactly the same marking, which showed a small crescent of white in the bubble. It appeared as though one ballot had been marked and then reproduced over 100 times. In addition, one of these ballots bore the distinctive ink markings of having been pulled from a printer too soon. Almost all of these ballots were votes for Vice President Biden; only two were for President Trump. In her 20 years of election experience, Voyles had never seen any ballots like these. As noted above, Ms. Voyles has been fired from her position as a poll manager with Fulton County, presumably for her honest testimony.

- Hal Soucie, who was also at the State Farm Arena, verified that he saw the pristine ballots mentioned by Ms. Voyles.

- During the recount, Scott Hall of Fulton County saw large quantities of ballots at the World Congress Center that appeared to have been machine-produced. He stated that he saw this "over and over." The Subcommittee received evidence that other poll workers throughout the State reported similar instances of "pristine" ballots with no explicable origin.

Duplication of Ballots Without Oversight

- Nancy Kain, a naturalized citizen in DeKalb County, volunteered as a poll watcher for Advance Voting at lower Roswell Road, served as a poll monitor during processing of absentee ballots and as a poll watcher on Election Day. At 10 a.m. on November 5, at the State Farm Arena, she was not asked for credentials and noticed that many people did not even have credentials. She observed a young man with paper ballots putting in selections on a ballot on a voting machine and wondered why it was not going through the scanner. The supervisor explained that the military ballots are transcribed in proper format and ballots come in that they were trying to salvage because of damage, thus they were just transferring them to a new ballot, and that was the process. Yet, no one was there to verify what the young man was doing. He was the brother of the

supervisor. Technically, he was voting for someone else on a voting machine. She took video and photographs and recorded her conversation with the supervisor.

- Mark Amick observed the processing of Provisional, Military and UOCAVA ballots in Fulton County on November 6 from early morning until 10:15 p.m. The only "oversight" provided was from a Secretary of State (SOS) employee who was not seen in the area before mid-morning, and who spent much of day not observing the duplication and tabulation process but rather sitting in the back of the room and leaving the room while on his phone. The first time Amick saw the SOS employee on the counting/sorting floor was 5:53 p.m. By 6:02 p.m. he had returned to his chair at the back of the room, and he did not go back onto the counting/sorting floor by the time Amick left at 10:15 p.m.

Denial of Entry to Election Day Poll Watchers and During Recount

- Mark Amick, a credentialed Statewide Poll Watcher in Milton (Fulton County), was denied entry into the Birmingham Falls Elementary School precinct despite his statewide credentials. The Subcommittee has also received evidence from monitors that some of them were denied entrance during the recount.

Hostility

- Hale Soucie of Symrna testified that Cobb County was using an electronic counting machine on the first day to count ballots, which was not the approved way to do the recount. The next day, it was the hand count process. He stated that on his second day he immediately observed that the first auditor made three mistakes in two minutes calling three ballots marked for Trump as Biden votes, but the second auditor caught those mistakes. He noticed another table that was not even doing a double-check at all. When he sought to observe, he was met with great hostility and vulgar name calling directed at him. The Subcommittee received other evidence of hostility against the monitors.

Wildly Disparate Vote Totals from the Recount

- While observing the recount at the DeKalb County Board of Elections on November 15, Mark Amick saw that a box of ballots was recorded as 10,707 votes for Biden and 13 votes for President Trump. He flagged this obvious disparity to the election workers, who discussed among themselves how it came to be. Two election officials with whom he engaged about this issue became agitated with Amick for his continued monitoring of the situation. They finally agreed to recount the box, resulting in a revised total of 1,081 votes for Vice President Biden and 13 for President Trump – still statistically disparate, but 9,626 votes less so. Amick was not certain if the corrected count was actually entered into the final recount totals.

- At State Farm Arena during the recount, Susan Voyles also noted a stack of absentee ballots with only two votes for President Trump.
- Hal Soucie of Smyrna, while monitoring in State Farm Arena, noticed stacks of ballots quite high, such as eight inches high for Biden, yet not a single Trump vote. He stated that he works with data and marketing, and anytime figures start reaching the 90th percentile, that type of consumer data is suspect, and when it gets to 100 percent that is passing the level of improbable to impossible.

Ballots Counted from Ineligible Voters

- Mark Davis analyzed data from U.S. Postal Service change-of-address (COA) forms and compared it to voters who voted in their former precincts. For example, he discovered that 14,980 out-of-state movers still voted in the Georgia General Election. Another 40,279 moved across county lines more than 30 days prior to the election, yet still voted in their former county precincts, a violation of Georgia law. He also noted that about 1,000 voters had voted twice in the Primary, inferring that the same pattern could have existed in the General Election.

Constitutional Violations of Duly Passed Law

- Dr. John C. Eastman, former Professor of Law and former Dean of the Chapman University Fowler School of Law and current Fellow at the Claremont Institute, testified regarding the plenary authority of the legislative body of the States to set the "Times, Places and Manner" of elections involving Federal officials, including with respect to the selection of Electors for the Electoral College in the presidential election, citing Article I, Section 4 and Article II, Section 1 of the U.S. Constitution. He noted that when States have vested that authority in the people of their States that they are bound to follow the people's choice in a free and fair election, but where fraud and failure to follow the law as passed by the legislative body is evident, that authority can be withdrawn. The legislature then can exercise its plenary authority to choose the electors in a presidential contest. He referenced both *Bush v. Gore* and *McPherson v. Blacker* as authoritative.

  Professor Eastman further explained that the failure of State election officials to follow the manner of conducting the election according to the statutes duly passed by the legislative body can annul an election. The U.S. Constitution clearly gives State legislatures under Article I, Section 4 the duty to determine the "manner" of federal elections, and that power rests solely with the State legislatures unless Congress passes its own laws that preempt State election laws. There is no provision which allows any Executive branch member to modify, set aside, enhance, or otherwise create policies or procedures which undermine or contravene those laws.

He noted various ways State election officials had failed to follow the statutes in conducting the election. He reiterated failures such as counting the votes of approximately 66,000 underage individuals, the 2,500 felons whose votes were unlawfully counted, the votes of those who had no verifiable residences within the State, and the "biggest" of all he believed was the March 2020 settlement agreement that was entered into with Georgia's Secretary of State and "certain democrat committee challengers that effectively altered the signature verification process" with regard to Absentee Ballots, an agreement that was contrary to State law. He further noted that the "intermingling of legal and illegal ballots" also meant that the election cannot legally be certified. "The State has failed to make a choice on Election Day in accordance with the manner" the legislature prescribed. In light of the failures, the fraud, and the unconstitutional agreement, Dr. Eastman opined that it was the duty of the legislative body to choose the State's Electors for the presidential election.

Data Analysis in General and Dominion Issues

- Russell J. Ramsland, Jr., a cybersecurity expert from Texas, testified that his team had compared data from Dominion voting machines in those places where they were used around the nation. They discovered that with Dominion machines, Vice President Biden outperformed what he was statistically expected to receive by an "amazing" 5%. He also outperformed statistical expectations when the analysis was run by county, with Vice President Biden picking up 78% of Dominion counties but only 46% of counties using machines from other manufacturers. Depending on the type of analysis performed, Ramsland estimated that these anomalies translated to between 123,000 and 136,000 extra votes for Vice President Biden in Georgia.

  Ramsland also found that the rejection rate for absentee ballots in Georgia was much lower in 2020 (0.2%) than in 2016 (6.4%). He also identified over 96,000 phantom votes, meaning that they had been counted, but there was no record of the counties recording those ballots as "received."

- Phil Waldron**,** a former U.S. Army information officer with expertise in electronic warfare, identified a "pretty significant information warfare campaign" conducted across the country during the Election. He described the history of the Dominion and other voting machines, with the operating software sharing the same "DNA" going back to Smartmatic, which was created to help steal elections in Venezuela.

  Waldron analyzed these machines in Michigan and found them extremely insecure. He said a good hacker could get into them within two minutes, while an elementary-school student could probably do it in twelve. There are 12 avenues of attack. Dominion also sends voter data outside the United States.

Waldron discussed fractional voting. Waldron testified that the Dominion software used in the Georgia machines assigns a fractional value to each vote; there is no legitimate purpose in assigning an elector's vote as a fractional vote. That feature can allow the manipulation of election results.

Waldron said federal law (USC Title 46) requires that the ballot images within the machine are required to be preserved for 22 months, but only a forensic analysis would show if this was done. Each machine can record 2,000-3,000 ballots per hour. His Michigan analysis showed "huge breaches in chain of custody" with respect to the machines and to absentee ballots. In Georgia, there was an unexplained upload of ballots at 3:36 a.m. on November 4.

Waldron urged a full forensic audit of the machines and of absentee ballots (for example, ink analysis would show if ballots were mass-produced).

- Scott Hall of Fulton County stated that when he worked at the English Street facility that he had concerns about the contractors hired there. He noted that every vote in Fulton County ends up on thumb drives that eventually find their way to the English Street location. He said, "I have photographs of pallet loads of basically signed checks." "So you've got every single vote, you've got currency, and now you just need someone to do it." He said he hired one of his own guys to determine if a fraudulent vote could be recorded on the Dominion machines at that point in the process. "Now, I've got all these votes that have not been uploaded anywhere. And he actually wrote me a paper, and he said that it was the 'stupidest, simplest thing I've ever seen.' He said, 'Dominion's own documentation shows how you take an entire batch, swipe it off, and then swipe on a new batch, before you put it into the real-time reader that uploads." He summed up the voter fraud by using the analogy that the referee got paid off to call the game and something is very wrong.

Outside Influence Over Governmental Election Functions

- Scott Walter from the Capitol Research Group testified about Mark Zuckerberg's Center for Technology and Civic Life (CTCL), a progressive advocacy group that seeks to influence elections via voter "education" and get-out-the-vote efforts. In the 2020 election, CTCL made grants to individual counties, in Georgia and elsewhere, ostensibly to help run safe elections during COVID. But county boards could use the money for whatever they wanted, and the bulk of the grants (95% of total funding) went to counties that voted for Clinton in 2016 and for Biden in 2020. In fact, nine of the 10 Georgia counties that experienced the largest shifts toward Democrats in 2020 received CTCL grants -- $4.38-$10.47 spent per each man, woman, and child in those counties. Georgia should not allow "privatized" elections via the organization that the Washington Post has called the "Democratic Party's Hogwarts for digital wizardry."

Voters Unable to Verify Votes Counted

- Grace Lennon, a student at Georgia Tech, hoped to early vote on October 23. When she arrived, she was told that she had been sent an absentee ballot. She never received an absentee ballot. She had to sign an affidavit saying that she had not requested nor had she received an absentee ballot. She was then given a voter card to vote on the machine. However, the next day, she learned that someone had voted absentee in her name on October 7th. She was not able to verify that her vote actually counted for the one she chose to select in the election or whether the absentee ballot counted instead. Senator Greg Dolezal confirmed that most all the Senators had heard many similar stories.

V. FINDINGS

1- The November 3, 2020 election was chaotic and the results cannot be trusted.
2- The Secretary of State and the State Elections Board failed to enforce the law as written in the Georgia Code, and furthermore, created policies that contravened State law. As Senator Matt Brass concluded at the December 3 hearing, "We have heard evidence that State law was not followed, time after time after time."
3- The Secretary of State failed to have a transparent process for the verification of signatures for absentee ballots, for the counting of votes during the subsequent recount and audit, and for providing the type of guidance and enforcement necessary to ensure that monitors and other observers had meaningful access to the process.
4- The Secretary of State instituted an unconstitutional gag order so that monitors were told not to use photography or video recording devices during the recount.
5- Election officials at all levels failed to secure test ballots and actual ballots. Many reports indicate that proper procedures were not followed, and there was systematic failure to maintain appropriate records of the chain of custody for these ballots, both prior to and after voting and throughout the recount.
6- The Secretary of State and Election Supervisors failed to stop hostile behavior of workers toward citizen volunteer monitors during the recount process.
7- The events at the State Farm Arena are particularly disturbing because they demonstrated intent on the part of election workers to exclude the public from viewing the counting of ballots, an intentional disregard for the law. The number of votes that could have been counted in that length of time was sufficient to change the results of the presidential election and the senatorial contests. Furthermore, there appears to be coordinated illegal activities by election workers themselves who purposely placed fraudulent ballots into the final election totals.
8- Grants from private sources provided financial incentives to county officials and exerted influence over the election process.
9- The oral testimonies of witnesses on December 3, 2020, and subsequently, the written testimonies submitted by many others, provide ample evidence that the 2020 Georgia General Election was so compromised by systemic irregularities and voter fraud that it should not be certified.

VI. RECOMMENDATIONS

A. Absentee Ballots

In addition to following the law as already written by the legislature, such as not opening absentee ballots until Election Day, additional steps should be taken to ensure that only legal absentee votes are counted.

At a minimum, these recommendations include requiring photo identification, following signature match procedures faithfully, allowing absentee ballots to be used only upon demonstration of need, mailing absentee ballots out only upon the request of the registered voter, and although already illegal, expressly prohibiting drop boxes.

B. Secure Chain of Custody and Additional Security Measures

Procedures should be established to ensure proper chain of custody for all ballots, whether they are test ballots, new unused ballots, spoiled ballots, cast BMD-generated ballots, absentee ballots, and even the specialty paper that is used to print the ballots.

Penalties should be clearly known and enforced for any violations.

There should be complete security when workers go on the job, with sign-in of their names and a time stamp, when they go in and when they go out.

Cameras should also be on-site to monitor the process at all times, as well as all the entrances to the buildings where ballots and the ballot paper are stored.

C. Meaningful Access for Poll Watchers and Monitors

Citizens who are seeking to ensure the integrity of the vote need to be able to truly see the process. They should be able to ensure that people are reading their ballots before they are cast. They should be able to inspect the signature match process when ballots are opened. They should be able to write down seal information so they can ensure proper custody is in place. They should be close enough to see the names on the ballots during any recounts, the counts written on recount report sheets, the counts going into the ARLO system, the counts written on ballot containers, the process of the seals being broken as the ballots are entering the process, and so forth.

More poll watchers and monitors should be allowed to participate since the ratio needs to be improved. Objections by monitors should be addressed immediately on-site to ensure access and transparency.

Hostile actions by election workers toward volunteers should be immediately addressed and should be cause for dismissal.

D. No Unconstitutional Gag Orders

There is no reason to ban cameras when tabulation is taking place or when recounts and audits are taking place.

Furthermore, there is no reason to ban cameras at the polling booth as long as voters have privacy while voting.

The State Board of Elections should not ban cameras and recording equipment. They must fulfill their duty to ensure a transparent election process. Furthermore, citizens have a right to share those photos, recordings, and thoughts about what they observe.

E. Unqualified Voters Should Be Purged from the System

No underage voters should be in the system to allow their votes. No felons should be in the system to allow their votes.

Other categories of voters, such as the deceased and those who have moved out of state, should also be examined as to their continued presence on the voter rolls.

F. Violations of State Election Laws Must Be Prosecuted

The Georgia Bureau of Investigation ("GBI") and the Attorney General should aggressively investigate and prosecute those who violate election laws, including those conspiring to place fraudulent ballots into the system and the 1,000 persons identified by the Secretary of State who voted twice in the 2020 primaries. If prosecutions do not happen, violations will recur.

The GBI should establish an independent office for the investigation of all claims of voter fraud. That office should report regularly to the Judiciary Committee and, except in the case of investigations involving the Secretary of State or its personnel, the office of the Secretary of State.

The GBI should investigate the cases where many affidavits already exist regarding election fraud in the 2020 General Election.

G. Forensic Audits of Ballots and Machines

The Legislature must determine if ballot marking devices (BMDs) have been manipulated to provide a fraudulent result and without regard to whether the forensic audits can actually identify the manipulation of votes and the authenticity of the ballots that are in the ballot boxes, either generated by the BMDs or those that are absentee ballots.

Independent third-party auditors should review the fiducials on all ballots types (absentee, military, machine generated), audit the absentee ballot results from the last election, confirm the number of external envelopes in each county, and the number of ballots for each county.

Such audits should help ensure that phantom ballots and other fraudulent ballots are not counted in election results, and that legal votes are the only votes counted.

H. For Rectifying the 2020 General Election Results

The Legislature should carefully consider its obligations under the U.S. Constitution. If a majority of the General Assembly concurs with the findings of this report, the certification of the Election should be rescinded and the General Assembly should act to determine the proper Electors to be certified to the Electoral College in the 2020 presidential race. Since time is of the essence, the Chairman and Senators who concur with this report recommend that the leadership of the General Assembly and the Governor immediately convene to allow further consideration by the entire General Assembly.

Respectfully submitted this the 30th day of December 2020.

EXHIBIT 9

Letter, Sen. William Ligon, Georgia State Senate, to Donald J. Trump (Jan. 2, 2021)

William Ligon
District 3
158 Scranton Connector
Brunswick, Georgia 31525
Office: 912.261.2263
Email: william@senatorligon.com

121-E State Capitol
Atlanta, Georgia 30334
Phone: 404.463.1383

William.Ligon@senate.ga.gov

Georgia Senate

Committees

Banking and Financial Institutions, Chairman
Ethics, Vice Chairman
Reapportionment and Redistricting, Vice Chairman
Appropriations
Health and Human Services
Judiciary

January 2, 2021

President Donald J. Trump
The White House
1600 Pennsylvania Ave.
Washington, DC 20500

Re: *Request for Assistance under the DHS Cyber Hunt And Incident Response Teams Act of 2019*

Dear Mr. President:

In accordance with DHS Cyber Hunt And Incident Response Teams Act of 2019, as Chairman of the Georgia Senate Judiciary Subcommittee on Elections (the "Committee"), I request that you immediately send an outside team of cyber experts to investigate potential hacking and other irregularities associated with Dominion Voting Systems, Inc.'s ("Dominion") scanners, ballot marking devices, ballots and polling pads used in the 2020 general election in Georgia.

On December 30, 2020, the Committee held a hearing investigating potential fraud and other irregularities during Georgia's 2020 general election. The Committee first unanimously approved a report dated December 17, 2020 discussing a myriad of voting irregularities and potential fraud in the Georgia 2020 general election (the "Report") discussed in an earlier hearing held on December 3, 2020. Notably, the Committee stated in the Executive Summary that "[t]he November 3, 2020 General Election (the 'Election') was chaotic and any reported results must be viewed as untrustworthy."[1]

The Committee then heard additional testimony concerning voting irregularities during the 2020 general election, including testimony and a real time test demonstrating serious irregularities with Dominion's voting machines. Three events discussed at this hearing stand out, and require a forensic audit of the Dominion voting machines in Georgia be immediately conducted.

---

[1] *See* http://www.senatorligon.com/THE_FINAL%20REPORT.PDF

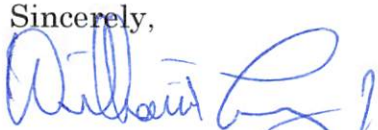
First, the Dominion voting machines employed in Fulton County had an astounding 93.67% error rate in the scanning of ballots requiring a review panel to "adjudicate" i.e. "determine" the voter's intent in over 106,000 ballots out of a total 113,130 ballots. The national average for such an error rate is far less at 1.2%. The source of this astronomical error rate must be identified to determine if these machines were set up or designed to allow for a third party to disregard the actual ballot cast by the registered voter.

Second, there is clear evidence that tens of thousands of votes were switched from President Trump to former Vice President Biden in several counties in Georgia. For example, in Bibb County, President Trump was reported to have 29,391 votes at 9:11 pm EST while simultaneously former Vice-President Joe Biden was reported 17,218 votes. Minutes later at the next update, these vote numbers switched with President Trump now having 17,218 votes and Mr. Biden having 29,391 votes, a 12,173 switch to Mr. Biden's favor. No rational explanation has been put forth demonstrating a legitimate reason for this switch in the vote tally.

Third, during this hearing, a presenter, Jovan Hutton Pulitzer, demonstrated that a Dominion poll pad could be hacked into real-time because it was connected to the internet. This demonstration proved that these machines could allow votes to be siphoned off or added during the voting process because they are connected to the internet. Cyber security experts agree that voting machines should not be connected to the internet at any time.

Former Vice President Biden leads in Georgia only by a margin of 11,779 votes. An immediate forensic audit of an appropriate sampling of Dominion's voting machines and related equipment is critical to determine the level of illegal or fraudulent ballots improperly counted in Georgia during the 2020 general election, and to safeguard future elections from such vulnerabilities. As of the date of this letter, a forensic audit of the Dominion voting machines has not occurred in Georgia. We, therefore, turn to you for relief at this critical moment in our Republic.

Sincerely,



William T. Ligon, Chairman
Senate Judiciary Subcommittee
on the Election

EXHIBIT 10

Genetski v. Benson, Case No. 20-000216-MM, (Mich. Ct. Claims, March 9, 2021)

STATE OF MICHIGAN

COURT OF CLAIMS

ROBERT GENETSKI, County of Allegan Clerk, individually and in his official capacity, and MICHIGAN REPUBLICAN PARTY,

Plaintiffs,

v

JOCELYN BENSON, in her official capacity, and JONATHAN BRATER, Director of Elections, in his official capacity,

Defendants.
_____/

OPINION AND ORDER GRANTING SUMMARY DISPOSITION IN PART TO PLAINTIFFS AND GRANTING SUMMARY DISPOSITION IN PART TO DEFENDANTS

Case No. 20-000216-MM

Hon. Christopher M. Murray

Before the Court is defendants' January 20, 2021 motion for summary disposition filed pursuant to MCR 2.116(C)(4) and (C)(8), as well as plaintiffs' February 3, 2021 cross-motion for summary disposition filed pursuant to MCR 2.116(C)(8). Plaintiffs' cross-motion will be GRANTED in part with respect to Count II of the amended complaint because the challenged signature-matching standards were issued in violation of the Administrative Procedures Act. As a result of the grant of summary disposition in plaintiffs' favor on Count II, Count I of the amended complaint will be dismissed without prejudice. In addition, defendants' motion for summary disposition will be GRANTED in part with respect to Counts III and IV of the amended complaint.

I. BACKGROUND

The issues raised implicate signature-matching requirements for absent voter ballot applications and absent voter ballot return envelopes contained in this state's election law. MCL

168.759 and MCL 168.761 require voters to sign applications for absent voter ballots in order to receive a ballot. In addition, this state's election laws require voters who choose to vote by absent voter ballot to sign their absent voter ballot return envelopes in order to have their ballots counted. MCL 168.764a. The signatures on the applications and the return envelopes are compared against signatures in the qualified voter file or those that appear on the "master registration card" in order to determine whether the signatures match. Signatures on applications or return envelopes that do not "agree sufficiently" with those on file are to be rejected. MCL 168.761(2). As of October 6, 2020, MCL 168.761(2)[1] was amended by 2020 PA 177 to give notice to voters' whose signatures do not "agree sufficiently" with those on file that their absent voter ballot application has been rejected. The purpose of the notice is to give voters the opportunity to correct inaccuracies with absent voter ballot signatures. The same notice requirements also apply to rejected signatures for absent voter ballots. MCL 168.765a(6). There is no dispute that this state's election law does not define what it means for signatures to "agree" or to "agree sufficiently" for purposes of comparing the signature on file with the signature on a received absent voter ballot application or absent voter ballot.

On the day PA 177 became effective, defendant Jocelyn Benson issued what defendants refer to as "guidance" for local clerks who are charged with inspecting signatures on absent voter ballot applications and ballots. The document, which was entitled "Absent Voter Ballot Processing: Signature Verification and Voter Notification Standards" largely mirrored guidance

[1] 2020 PA 302 further amended MCL 168.761 and other provisions of this state's election law. Those amendments do not become effective until June 27, 2021. This opinion and order only examines those provisions of the statute that are currently in effect at this time. And no issues have been raised with respect to the yet-to-be-effective statutory requirements.

defendant Benson had previously issued. This guidance regarding signature verification forms the heart of the issues in the present case and it requires additional examination.

The stated purpose of the at-issue document was to "provide[ ] standards" for reviewing signatures, verifying signatures, and curing missing or mismatched signatures. Under a heading entitled "Procedures for Signature Verification," the document stated that signature review "begins with the presumption that" the signature on an absent voter ballot application or envelope is valid. Further, the form instructs clerks to, if there are "any redeeming qualities in the [absent voter] application or return envelope signature as compared to the signature on file, treat the signature as valid." (Emphasis in original). "Redeeming qualities" are described as including, but not being limited to, "similar distinctive flourishes," and "more matching features than nonmatching features." Signatures "should be considered questionable" the guidance explained, only if they differ "in multiple, significant and obvious respects from the signature on file." (Emphasis in original). "[W]henever possible," election officials were to resolve "[s]light dissimilarities" in favor of finding that the voter's signature was valid.[2]

The section on signature-verification procedures goes on to repeat the notion that "clerks should presume that a voter's [absent voter] application or envelope signature is his or her genuine signature, as there are several acceptable reasons that may cause an apparent mismatch." (Emphasis omitted). Next, the guidance gave excuses or hypothetical explanations for why signatures on absent voter ballot applications and absent voter ballots might not be an exact match to those that are on file. Finally, the document again mentioned the presumption when, in

[2] The guidance included a chart with what were deemed to be acceptable and unacceptable "defects" in signatures.

conclusion, it stated that clerks "*must perform* their signature verification duties with the presumption that the voter's [absent voter] application or envelope signature is his or her genuine signature." (Emphasis added). By all accounts, the guidance set forth in that document was not limited to the then-upcoming November 2020 general election, nor has it been rescinded. Rather, it appears that the guidance remains in effect for local clerks with respect to upcoming elections.

II. PLAINTIFFS' COMPLAINT

Plaintiff Robert Genetski is the Allegan County Clerk. He, along with plaintiff Michigan Republican Party, filed a complaint alleging that defendant Benson's October 6, 2020 guidance is unlawful. The December 30, 2020 amended complaint alleges that the presumption in favor of finding valid signatures is unlawful, as is the directive to find "any redeeming qualities" for signatures. They contend that the presumption contained in the guidance issued by defendant Benson will allow invalid votes to be counted. Plaintiff Genetski has not, however, alleged that this guidance caused him to accept a signature that he believed was invalid.

The four-count amended complaint asks the Court to issue declaratory and injunctive relief with respect to future elections. Count I alleges that defendant Benson violated various provisions of this state's election law by issuing the challenged guidance regarding signature-matching requirements which allegedly conflicts with this state's election law. They ask the Court to issue injunctive relief to remedy the allegedly unlawful guidance. Additionally, they seek a declaratory ruling regarding the validity of defendant Benson's guidance.

Count II of the amended complaint alleges that defendant Benson's guidance was a "rule" as defined by the Administrative Procedures Act (APA) that was issued without compliance with the APA. Plaintiffs allege that the guidance is in fact a rule because it is generally applicable and

requires local election officials to apply a mandatory presumption of validity to signatures. Plaintiffs ask the Court to declare that the "rule" is invalid.

Count III alleges a violation of Const 1963, art 1, §§ 2 and 5, as defendant Benson's guidance will result in the counting of invalid absent voter ballots which will ultimately result in the dilution of valid votes cast by this state's electorate. They argue that defendant Benson's guidance is so vague and imprecise that it cannot be applied uniformly throughout the state.[3]

Count IV alleges that plaintiff Genetski had a right to request an audit of his choosing under Const 1963, art 2, § 4(1)(h) as it relates to absent voter ballots. Plaintiffs acknowledge that defendants have announced and/or completed a state-wide audit of the November 2020 general election; however, according to plaintiffs, the audit does not address plaintiffs' concerns because it did not review whether signatures on absent voter ballots were properly evaluated. Plaintiffs ask the Court to declare that the right to request an audit under art 2, § 4(1)(h) encompasses the type of absent-voter-ballot review requested in the amended complaint. Plaintiff also suggests the manner in which such an audit should be conducted.

III. ANALYSIS

A. MOOTNESS AND RIPENESS

Defendants argue that this Court should refrain from evaluating the merits of plaintiffs' complaint because the issues are either moot or not ripe. With respect to mootness, there is no dispute that Count III, which raises an equal protection claim arising out of the November 2020

[3] Plaintiffs' briefing has conceded that this claim is now moot, with the November 2020 election having already come and gone. As a result, the Court will not address this claim in any additional detail.

general election, is moot and must be dismissed. However, the Court declines to find that plaintiffs' remaining challenges are either moot or not ripe. Those issues concern the validity of guidance that is still in effect (Counts I and II), or an audit (Count IV) that, according to the plain text of art 2, § 4(1)(h) and MCL 168.31a, may be requested after the election has occurred. Moreover, defendants have not advanced a specific mootness/ripeness argument with respect to the audit claim. As a result, the Court declines to find that the issues raised in Counts I, II, and IV of the amended complaint would have no practical effect on an existing controversy or that it would be impossible to render relief. Cf. *Garrett v Washington*, 314 Mich App 436, 449-450; 886 NW2d 762 (2016) (describing the mootness doctrine).

The Court also rejects defendants' contention that there is no actual controversy. As noted, plaintiffs seek declaratory relief. MCR 2.605(A)(1) requires that there be "a case of actual controversy" for the issuance of declaratory relief. "In general, 'actual controversy' exists where a declaratory judgment or decree is necessary to guide a plaintiff's future conduct in order to preserve his legal rights." *Shavers v Kelley*, 402 Mich 554, 588; 267 NW2d 72 (1978). Here, plaintiffs—particularly plaintiff Genetski, who is a local clerk subject to the guidance at issue—sought a declaration regarding whether he is and will continue to be subject to guidance that by all accounts remains in effect at this time. This clearly presents an actual controversy that is appropriate for declaratory relief. See *id*.

Defendants argue that no actual controversy exists because the Legislature could change the applicable law, or because defendant Benson could decide to revoke the guidance. That argument would seek to turn the requirements of declaratory relief on their head and would eviscerate the purpose of declaratory relief. If the Court were to adopt the view that no actual controversy exists because the law could change, there could be no limit to the number of cases

that could be dismissed as moot. Here, plaintiffs have sought a declaration as to their legal rights with respect to the validity of a currently existing directive issued by defendant Benson in advance of the next election. That the law could hypothetically change in the future is not a reason to avoid issuing a declaration of the parties' currently existing legal rights, as plaintiffs have sought here. Indeed, the ability to seek an advance declaration of legal rights on an existing policy is one of the very reasons why the declaratory judgment rule was adopted in the first instance. See *UAW v Central Mich Univ Trustees*, 295 Mich App 486, 496; 815 NW2d 132 (2012) (discussing the purposes of the declaratory judgment rule).

B. WHETHER DEFENDANT'S ACTIONS VIOLATED THE APA

The dispositive issue, as the Court see it, concerns the APA and whether defendant Benson was required to comply with the APA when she issued the "Signature Verification and Voter Notification Standards." The Secretary of State has authority, under MCL 168.31(1)(a), to "issue instructions and promulgate rules pursuant to the administrative procedures act of 1969, 1969 PA 306, MCL 24.201 to 24.328, for the conduct of elections and registrations in accordance with the laws of this state." Under the APA, a "rule" is defined as "an agency regulation, statement, standard, policy, ruling, or instruction of general applicability that implements or applies law enforced or administered by the agency, or that prescribes the organization, procedure, or practice of the agency, including the amendment, suspension, or rescission of the law enforced or administered by the agency."[4] MCL 24.207. A "rule" not promulgated in accordance with the

[4] There is no dispute that defendant Benson is subject to the APA, generally. See MCL 24.203(2) (defining "agency" in a way that includes the Secretary of State). The only dispute is whether this particular action is subject to the APA.

APA's procedures is invalid. MCL 24.243; MCL 24.245; *Pharris v Secretary of State*, 117 Mich App 202, 205; 323 NW2d 652 (1982).

An agency must utilize formal APA rulemaking procedures when establishing policies that "do not merely interpret or explain the statute or rules from which the agency derives its authority," but rather "establish the substantive standards implementing the program." *Faircloth v Family Indep Agency*, 232 Mich App 391, 403-404; 591 NW2d 314 (1998). "[I]n order to reflect the APA's preference for policy determinations pursuant to rules, the definition of 'rule' is to be broadly construed, while the exceptions are to be narrowly construed." *AFSCME v Dep't of Mental Health*, 452 Mich 1, 10; 550 NW2d 190 (1996). It is a question of law whether an agency policy is invalid because it was not promulgated as a rule under the APA. *In re PSC Guidelines for Transactions Between Affiliates*, 252 Mich App 254, 263; 652 NW2d 1 (2002).

As for whether the guidance or directive at issue is a "rule" subject to the APA, the Court must look beyond the labels used by the agency and make an independent determination of whether the action taken by the agency was permissible or whether it was an impermissible rule that evaded the APA's requirements. *AFSCME*, 452 Mich at 9. In other words, the Court "must review the actual action undertaken by the directive, to see whether the policy being implemented has the effect of being a rule." *Id*. (citation and quotation marks omitted).

Examining the "Signature Verification and Voter Notification Standards" through that lens, the Court agrees with plaintiffs that the same constitutes a "rule" that should have been promulgated pursuant to the APA's procedures. The standards are generally applicable to all absent voter ballot applications and absent voter ballots, and it contains a mandatory statement from defendant, this state's chief election officer, see MCL 168.21, declaring that all local clerks

"*must perform* their signature verification duties" in accordance with the instructions. (Emphasis added). In addition, clerks must presume that signatures are valid. That this presumption is mandatory convinces the Court that it is not merely guidance, but instead is a generally applied standard that implements this state's signature-matching laws. See MCL 24.207 (defining "rule"); *AFSCME*, 451 Mich at 8 (describing what constitutes a "rule" under the APA); *Spear v Mich Rehab Servs*, 202 Mich App 1, 5; 507 NW2d 761 (1993) (focusing on the mandatory nature of policies in support of the conclusion that the same constituted a "rule" under the APA).

Defendants cite three statutory exceptions to rulemaking—MCL 24.207(g), (h), and (j)—but the Court is not persuaded that the standards are saved by any of these exceptions. The first argument is that MCL 24.207(j), which is sometimes referred to as the "permissive power exception," applies and exempts the standards from the APA's rulemaking requirements. MCL 24.207(j) exempts from the APA's definition of "rule," a "decision by an agency to exercise or not to exercise a permissive statutory power, although private rights or interests are affected." Here, defendant Benson points to MCL 168.31(1)(a) as the source of her "permissive statutory power." That statute provides that the Secretary of State "shall" "issue instructions and promulgate rules pursuant to the administrative procedures act of 1969, 1969 PA 306, MCL 24.201 to 24.328, for the conduct of elections and registrations in accordance with the laws of this state." MCL 168.31(1)(a). According to defendant Benson, MCL 168.31(1)(a) allows her to eschew the rule-making process in order to issue "instructions" like the standards at issue.

The Court disagrees. First, the Court disagrees with defendants' characterization of the standards at issue, for the reasons stated above. Second, the cited statutory authority requires defendant Benson to issue instructions that are "in accordance with the laws of this state." MCL 168.31(1)(a). Here, it is not apparent that the mandatory presumption of signature validity is "in

accordance with the laws of this state."[5] To that end, nowhere in this state's election law has the Legislature indicated that signatures are to be presumed valid, nor did the Legislature require that signatures are to be accepted so long as there are any redeeming qualities in the application or return envelope signature as compared with the signature on file. Policy determinations like the one at issue—which places a thumb on the scale in favor of a signature's validity—should be made pursuant to properly promulgated rules under the APA or by the Legislature. See *AFSCME*, 452 Mich at 10.

Third, a review of the plain language of MCL 168.31(1) and of caselaw discussing the permissive-power exemption does not support defendants' argument.[6] The primary problem with defendant Benson's argument is that the language in MCL 168.31(1) is too generic to support her positions. MCL 168.31(1)(a) simply states that the secretary shall "issue instructions and promulgate rules pursuant to the" APA "for the conduct of elections." If that were sufficient to constitute an explicit or implicit grant of authority to be excepted from the APA rule-making process, then defendants would never have to issue APA-promulgated rules for any election-related matters. This view, where the exception would effectively swallow the rule, does not find support in caselaw. See, e.g., *AFSCME*, 452 Mich at 12. That is, while defendant has statutory discretion to decide whether to take certain actions, the implementation of her discretionary decisions—absent a more precise directive than is contained in the statutes at issue—

[5] Given that the standards are invalid for being enacted without compliance with the APA, the Court declines, for now, to determine whether the mandatory presumption imposed is contrary to the law, as plaintiffs have alleged in Count I. Resolution of that issue becomes unnecessary in light of the decision to grant relief to plaintiffs on Count II of the complaint.

[6] The Court incorporates and restates its reasoning and discussion of a similar issue from *Davis v Benson*, (Docket Nos. 20-000207-MZ & 20-000208-MM).

must still adhere to the APA if that implementation takes the form of a rule. See *id*. (recognizing that the Department of Mental Health did not need to take a certain action; however, once the Department exercised its discretion to act, the implementation of the decision "must be promulgated as a rule."); *Spear*, 202 Mich App at 5 (holding that while the agency's "decision to employ a needs test represents the discretionary exercise of statutory authority exempt from the definition of a rule under [MCL 24.207(j)], the test itself, which is developed by the agency, is not exempt from the definition of a rule and, therefore, must be promulgated as a rule in compliance with the Administrative Procedures Act."). Thus, while defendant Benson undoubtedly has discretion under MCL 168.31 to issue guidance or to instruct local clerks regarding signature validity requirements, the implementation of her discretionary decision can still be subject to the APA's requirements.

Furthermore, the caselaw relied on by defendants in arguing for a different conclusion is easily distinguishable, and, in some cases, even lends support for the Court's conclusion. See e.g., *Detroit Base Coalition for Human Rights of Handicapped v Dep't of Social Servs*, 431 Mich 172, 187-188; 428 NW2d 335 (1988); *Mich Trucking Ass'n v Mich Pub Serv Comm*, 225 Mich App 424, 430; 571 NW2d 734 (1997); *By Lo Oil Co v Dep't of Treasury*, 267 Mich App 19, 47; 703 NW2d 822 (2005). In the cases cited above, the pertinent agency's enabling statute expressly or impliedly authorized the specific action later taken by the administrative agency; additionally, and significantly, those statutes also permitted the specific action to be achieved either through rulemaking *or* other means. See *Detroit Base Coalition*, 428 Mich at 187-188 ("The situations in which courts have recognized decisions of [an agency] as being within the [MCL 24.207(j)] exception are those in which explicit or implicit authorization for the actions in question has been found."). Here, MCL 168.31(1) provides generalized authority to defendant, and it lacks

specificity with respect to the action taken (implementation of a mandatory presumption of signature validity), making the statute distinguishable from the statutes at issue in cases such as *Detroit Base Coalition, Mich Trucking Ass'n*, and *By Lo Oil Co.*[7]

Defendants raise concerns that this Court's interpretation of MCL 168.31(1)(a) would leave the term "instructions" without any practical effect. According to defendants, this Court's view would raise questions regarding whether defendant Benson could do anything when advising and directing local election officials as to the proper methods of conducting elections. The Court disagrees with the premise of defendants' position because, regardless of what is permissible under MCL 168.31, it is apparent that that which occurred here is not permissible, absent compliance with the APA. Here, defendant issued a mandatory directive and required local election officials to apply a presumption of validity to all signatures on absent voter ballot applications and on absent voter ballots. The presumption is found nowhere in statute. The mandatory presumption goes beyond the realm of mere advice and direction, and instead is a substantive directive that adds to the pertinent signature-matching statutes. And for similar reasons, defendants' arguments about efficiency and the need for quick action do not change the Court's decision. That is, nothing about the Court's opinion should be read as limiting the Secretary of State's ability to take quick action when she so desires. However, when that action takes the form of a rule, then the APA and MCL 168.31 require that the APA be invoked. In other words, the statute gives the Secretary of State

[7] Remarkably, defendants continue to place reliance on the conclusions of the majority in *Pyke v Dep't of Social Servs*, 182 Mich App 619; 453 NW2d 274 (1990). But as noted in prior opinions, Judge Shepard's dissent in *Pyke* was later adopted by the *Palozolo* Court, and as that Court noted, its decision was binding under what is now MCR 7.215(J)(1). *Palozolo v Dep't of Social Servs*, 189 Mich App 530, 533-534 & n 1; 473 NW2d 765 (1991). The *Pyke* Court's view on MCL 24.207(j) is irrelevant.

the authority and the ability to meet the needs of a situation. But when the action taken constitutes a "rule" under MCL 24.207, the appropriate procedures must be followed.

Defendants' citation to the rule-making exceptions contained in MCL 24.207(g) and (h)—which are the primary exemptions cited in their reply briefing—are no more convincing. Turning first to MCL 24.207(g), this subsection is an exception to the APA's rule-making requirements for an "intergovernmental, interagency, or intra-agency memorandum, directive, or communication that does not affect the rights of, or procedures and practices available to, the public." This exception is inapplicable, however, because the at-issue standard involves a mandatory presumption that directly affects local election officials' duties with respect to the determination of whether a voter's signature on either an absent voter ballot or a returned ballot will be deemed to be valid. Cf. *Kent Co Aeronautics Bd v Dep't of State Police*, 239 Mich App 563; 609 NW2d 593 (2000) (finding that a directive fit within the exception where it did not create any obligations or require compliance).

Nor is defendants' citation to the exception contained in MCL 24.207(h) convincing. That exception applies to a "form with instructions, an interpretive statement, a guideline, an informational pamphlet, or other material that in itself does not have the force and effect of law but is merely explanatory." MCL 24.207(h). This exception "must be narrowly construed and requires that the interpretive statement at issue be merely explanatory." *Clonlara, Inc v State Bd of Ed*, 442 Mich 230, 248; 501 NW2d 88 (1993) (citation and quotation marks omitted). If the purported "interpretive" statement changes the requirements of the law it is alleged to have interpreted, the exception does not apply. *Id*. See also *Schinzel v Dep't of Corrections*, 124 Mich App 217, 221; 333 NW2d 519 (1983). Here, because nothing in this state's election law refers to a presumption of validity, let alone a mandatory presumption, the standards at issue cannot be

deemed to be merely explanatory. See *Clonlara*, 442 Mich at 248, 251. That is, rather than merely explaining existing obligations under the law, the standards have imposed new obligations that do not appear within the plain language of this state's signature-matching statutes.

In sum, the standards issued by defendant Benson on October 6, 2020, with respect to signature-matching requirements amounted to a "rule" that should have been promulgated in accordance with the APA. And absent compliance with the APA, the "rule" is invalid. Whether defendant Benson had authority to implement that which she did not need not be decided at this time because it is apparent the APA applied to the type of action taken in this case. Accordingly, plaintiffs are entitled to summary disposition on Count II of the complaint, and the Court will dismiss Count I without prejudice as a result.

C. PLAINTIFFS' AUDIT CLAIMS ARE WITHOUT MERIT

Finally, the Court examines Count IV of the complaint, which concerns plaintiffs' request for an audit. Const 1963, art 2, § 4(1)(h), provides that a qualified Michigan voter has the right to have "*the results* of statewide elections audited" in a manner prescribed by law. (Emphasis added). MCL 168.31a, amended after adoption of the aforementioned audit language, provides as follows:

> (1) In order to ensure compliance with the provisions of this act, after each election the secretary of state may audit election precincts.
>
> (2) *The secretary of state shall prescribe the procedures for election audits* that include reviewing the documents, ballots, and procedures used during an election as required in section 4 of article II of the state constitution of 1963. *The secretary of state and county clerks shall conduct election audits, including statewide election audits, as set forth in the prescribed procedures*. The secretary of state shall train and certify county clerks and their staffs for the purpose of conducting election audits of precincts randomly selected by the secretary of state in their counties. *An election audit must include an audit of the results of at least 1 race in each precinct selected for an audit. A statewide election audit must include an audit of the results*

> *of at least 1 statewide race or statewide ballot question in a precinct selected for an audit*. An audit conducted under this section is not a recount and does not change any certified election results. The secretary of state shall supervise each county clerk in the performance of election audits conducted under this section.
>
> (3) Each county clerk who conducts an election audit under this section shall provide the results of the election audit to the secretary of state within 20 days after the election audit. [Emphasis added.]

Plaintiffs acknowledge that an audit of the November 2020 general election results was conducted. They argue that they have the right to request an audit with respect to the subject of their choosing—signatures on absent voter ballot applications and on absent voter ballots—and in the manner of their choosing. For at least two reasons this claim is not supported by art 2, § 4 or the implementing statute, MCL 168.31a. First, the constitution speaks of an audit of election *results*, not signature-matching procedures. Second, while the statute allows for an audit that includes "reviewing the documents, ballots, and procedures" used in the election, the statute plainly leaves it to the Secretary of State to "prescribe the procedures for election audits" and mandates that the Secretary of State shall conduct audits "as set forth in the prescribed procedures." In other words, there is no support in the statute for plaintiffs to demand that an audit cover the subject of their choosing or to dictate the manner in which an audit is conducted. MCL 168.31a(2) leaves that to the Secretary of State. As a result, plaintiffs have failed to state a claim on which relief can be granted as it concerns Count IV, and this count will be dismissed with prejudice pursuant to MCR 2.116(C)(8).

IV. CONCLUSION

IT IS HEREBY ORDERED that pursuant to MCR 2.116(C)(10), plaintiffs' cross-motion for summary disposition is GRANTED in part with respect to Count II of the amended complaint because the guidance issued by the Secretary of State on October 6, 2020, with respect to signature-matching standards was issued in violation of the Administrative Procedures Act.

IT IS FURTHER ORDERED that pursuant to MCR 2.116(C)(8) defendants' motion for summary disposition is GRANTED in part on Counts III and IV of the amended complaint.

IT IS FURTHER ORDERED that Count I of the amended complaint is dismissed without prejudice, for the reason that the at-issue standards are invalid under the Administrative Procedures Act.

This is a final order that resolves the last pending claim and closes the case.

Date: March 9, 2021

Christopher M. Murray
Judge, Court of Claims

EXHIBIT 11

Affidavit of Jessy Jacob (Nov. 7, 2020)

RECEIVED by MSC 11/26/2020 2:44:13 AM

GREAT LAKES JUSTICE CENTER

STATE OF MICHIGAN

IN THE CIRCUIT COURT FOR THE COUNTY OF WAYNE

CHERYL A. COSTANTINO and EDWARD P. McCALL, JR.,

Plaintiff,

-vs-

CITY OF DETROIT; DETROIT ELECTION COMMISSION; JANICE M. WINFREY, in her official capacity as the CLERK OF THE CITY OF DETROIT and the Chairperson of the DETROIT ELECTION COMMISSION; CATHY M. GARRETT, in her official capacity as the CLERK OF WAYNE COUNTY; and the WAYNE COUNTY BOARD OF CANVASSERS,

Defendants.

AFFIDAVIT OF JESSY JACOB

FILE NO: 20-_____-AW

JUDGE

David A. Kallman (P34200)
Erin E. Mersino (P70886)
Jack C. Jordan (P46551)
Stephen P. Kallman (P75622)
GREAT LAKES JUSTICE CENTER
Attorneys for Plaintiff
5600 W. Mount Hope Hwy.
Lansing, MI 48917
(517) 322-3207/Fax: (517) 322-3208

AFFIDAVIT

The Affiant, Jessy Jacob, being first duly sworn, hereby deposes and states as follows:

1. My name is Jessy Jacob. I am an adult citizen and resident of the State of Michigan.
2. I have been an employee for the City of Detroit for decades.
3. I was assigned to work in the Elections Department for the 2020 election.
4. I received training from the City of Detroit and the State of Michigan regarding the election process.

RECEIVED by MSC 11/26/2020 2:44:13 AM

GREAT LAKES JUSTICE CENTER

5. I worked at the election headquarters for most of September and I started working at a satellite location for most of October, 2020.

6. I processed absentee ballot packages to be sent to voters while I worked at the election headquarters in September 2020 along with 70-80 other poll workers. I was instructed by my supervisor to adjust the mailing date of these absentee ballot packages to be dated earlier than they were actually sent. The supervisor was making announcements for all workers to engage in this practice.

7. At the satellite location, I processed voter registrations and issued absentee ballots for people to vote in person at the location.

8. I directly observed, on a daily basis, City of Detroit election workers and employees coaching and trying to coach voters to vote for Joe Biden and the Democrat party. I witnessed these workers and employees encouraging voters to do a straight Democrat ballot. I witnessed these election workers and employees going over to the voting booths with voters in order to watch them vote and coach them for whom to vote.

9. During the last two weeks while working at this satellite location, I was specifically instructed by my supervisor not to ask for a driver's license or any photo I.D. when a person was trying to vote.

10. I observed a large number of people who came to the satellite location to vote in-person, but they had already applied for an absentee ballot. These people were allowed to vote in-person and were not required to return the mailed absentee ballot or sign an affidavit that the voter lost the mailed absentee ballot.

11. Whenever I processed an absentee voter application or in-person registration, I was instructed to input the person's name, address, and date of birth into the Qualified Voter File (QVF) system.

12. The QVF system can be accessed and edited by any election processor with proper credentials in the State of Michigan at any time and from any location with internet access.

13. I worked at the satellite location until the polls closed on November 3, 2020 at 8:00 p.m. and properly completed the entry of all absentee ballots into the QVF by 8:30 p.m.

RECEIVED by MSC 11/26/2020 2:44:13 AM

GREAT LAKES JUSTICE CENTER

14. I then reported to work at the TCF Center on November 4, 2020, at 8:30 a.m. to process ballots. I was instructed not to validate any ballots and not to look for any deficiencies in the ballots.

15. Absentee ballots that were received in the mail would have the voter's signature on the envelope. While I was at the TCF Center, I was instructed not to look at any of the signatures on the absentee ballots, and I was instructed not to compare the signature on the absentee ballot with the signature on file.

16. All absentee ballots that existed were required to be inputted into the QVF system by 9:00 p.m. on November 3, 2020. This was required to be done in order to have a final list of absentee voters who returned their ballots prior to 8:00 p.m. on November 3, 2020. In order to have enough time to process the absentee ballots, all satellites were instructed to collect the absentee ballots from the drop-box once every hour on November 3, 2020.

17. On November 4, 2020, I was instructed to improperly pre-date the absentee ballots receive date that were not in the QVF as if they had been received on or before November 3, 2020. I was told to alter the information in the QVF to falsely show that the absentee ballots had been received in time to be valid. I estimate that this was done to thousands of ballots.

18. The above information is true to the best of my information, knowledge, and belief.

19. Further affiant says not.

Jessy Jacob

On this 7th day of November, 2020, before me personally appeared Jessy Jacob, who in my presence did execute the foregoing affidavit, and who, being duly sworn, deposes and states that she has read the foregoing affidavit by her subscribed and knows the contents thereof, and that the same is true of her own knowledge and belief, except as to those matters she states to be on information and belief, and as to those matters she believes them to be true.

Stephen P. Kallman
Notary Public, Eaton County, Michigan
My Commission Expires: 11/26/2025

EXHIBIT 12

Affidavit of William Hartman (Nov. 18, 2020)

AFFIDAVIT

The Affiant, William C. Hartmann, being first duly sworn, hereby deposes and states as follows:

1. My name is William C. Hartmann. I am an adult citizen, voter, and resident of the State of Michigan.
2. I am a member of the Board of Canvassers of Wayne County, Michigan.
3. I personally observed the Absent Voter Counting Boards in Detroit at TCF Center.
4. Since the election on November 3rd, I have attended the Wayne County Canvass on an almost daily basis.
5. On November 17, 2020, at 3:00 p.m. there was a meeting of the Board of Canvassers to determine whether to certify the results of Wayne County. The meeting did not start until 5:00 p.m. We were told it was delayed so that representatives of the Democrat Board members could obtain additional affidavits.
6. At 5:00 p.m. an open meeting and discussion began to discuss the issue of whether to certify the vote. In my review of the results, I determined that approximately 71% of Detroit's 134 Absent Voter Counting Boards (AVCB) were left unbalanced and many *unexplained.* I informed the Board members of the discrepancies, but soon thereafter, a motion to certify was

made by Vice-Chairman Jonathan Kinloch. After further discussion, I renewed my concerns that the reason that the numbers did not balance for the majority of AVCB's in Detroit, and importantly, could not be explained. If the vote totals did not match, there should have been a documented reason explaining why.

7. The Board considered the ultimate question of whether to certify the vote, and the motion to certify the Wayne County elections failed 2-2.
8. This vote was followed by public derision from our two democrat colleagues. I, and Monica Palmer, who also voted against certification, were berated and ridiculed by members of the public and other Board members. This conduct included specious claims that I was racially motivated in my decision. This public ostracism continued for hours during which time we were not provided an opportunity to break for dinner and were not advised that we could depart and resume the hearing on another date.
9. I discussed a potential resolution with Vice-Chair Kinloch in confidence. Ms. Anderson-Davis told us that we must vote to certify on that night. We were told that we could not consider matters such as the unexplained reasons that most of Detroit's AVCB's did not balance and no one knew why. We

were informed that this consideration was outside of the scope of the Board's authority.

10. During the evening, Wayne County counsel, Ms. Janet Anderson-Davis, and my colleagues on the Board, continued to discuss irregularities in the AVCB's. Ms. Anderson-Davis advised the Board that the discrepancies were not a reason to reject the certification, and based on her explicit legal guidance, I was under the belief that I could not exercise my independent judgment in opposition to the certification. Therefore, I voted to certify the results.

11. Late in the evening, I was enticed to agree to certify based on the promise that a full and independent audit would take place. I would not have agreed to the certification but for the promise of an audit.

12. Vice-Chairman Jonathan Kinloch then assured us that if we voted to certify the election, a full, independent, and complete audit of Detroit's election, would be undertaken. We relied on this assurance in coming to an agreement. Without this assurance, I would not have agreed to certify Wayne County on November 17th.

13. After the meeting, I was made aware that Michigan Secretary of State, Jocelyn Benson made a public claim that the representations made by Mr. Kinlock, on which we had relied, would not be followed.

c. I am also concerned about the use of private monies directing local officials regarding the management of the elections, how those funds were used and whether such funds were used to pay election workers. I have not received answers to these questions, and I believe the people of Michigan deserve these answers. Can we release the logs to the tabulators demonstrating what happened in Detroit?

d. Why do the pollbooks, Qualified Voter Files, and final tallies not match or balance?

e. 71% of Detroit AVCB's did not balance, why not?

f. Did the chairperson of each of Detroit's 134 AVCB's keep logs of shift changes?

g. Why were republicans *not* used in signing seals certified at the end of the night on Monday, and Wednesday evening before ballot boxes were documented, closed, and locked?

h. How many challenged ballots were counted?

i. Was any information placed directly into the Qualified Voter Files in the AVCB's?

j. How many voter birthdates were altered in the pollbooks?

k. Were ballots counted in TCF that were not reflected in the electronic pollbook or paper supplemental list?

l. Based upon information and belief, there were over 18,000 same-day registrations in Detroit on November 3. Were these new applicants verified as proper voters prior to the tabulation of their ballots?

18. I voted not to certify, and I still believe this vote should *not* be certified.

19. Until these questions are addressed, I remain opposed to certification of the Wayne County results.

19. The above information is true to the best of my information, knowledge, and belief.

I certify under penalty of perjury, that my statement and the evidence submitted with it, are all true and correct.

Printed Name: William C. Hartmann

Signed Name: [signature]

Date:

Sworn to before me this 18th day of November, 2020 at 6:29pm

Melissa Wojnar-Raycraft
Notary Public Melissa Wojnar-Raycraft

My Commission expires on: Feb. 9, 2023

Melissa Wojnar-Raycraft
NOTARY PUBLIC - STATE OF MICHIGAN
COUNTY OF WAYNE
MY COMMISSION EXPIRES FEBRUARY 9, 2023
ACTING IN THE COUNTY OF Wayne

EXHIBIT 13

Affidavit of Monica Palmer (Nov. 18, 2020)

AFFIDAVIT

I, Monica Palmer, being first duly sworn, and under oath, state:

1. I am the Chairperson of the Wayne County Board of Canvassers.
2. The Board is a four-member board, required to have two Republican and two Democrat members, and I serve as one of the Republican members.
3. On August 4, 2020, the Michigan primary election was held.
4. On August 18, 2020, the Board held a public meeting at the Board's office in Detroit. I attended the meeting with the other three members of the Board.
5. The Board reviewed the Wayne County election results and considered whether to certify the August 4, 2020 primary election.
6. As reflected in the meeting minutes, Wayne County Election Director Gregory Mahar gave the Board a report at the meeting that included the following findings:
    - Staff encountered difficulties while trying to canvass the City of Detroit absentee precincts. "He indicated that aside from receiving the poll books on the first Friday and Sunday after the canvass began, the list of voters received made it difficult to determine how many voters actually returned their ballot. He reported that the City of Detroit used the QVF printed list of voters but there was also a handwritten list of voters, which is common to use both, but the two lists combined put the precincts severely out of balance."
    - "Director Mahar also reported on the difficulties staff encountered with trying to retabulate any absentee precincts that were out of balance. He stated that according to the Election Management system, he could see the City of Detroit did not scan a single precinct within a batch. When multiple precincts are scanned within a batch, it makes it nearly impossible to retabulate a precinct without potentially disrupting a perfectly balanced precinct."
    - "Deputy Director Jennifer Redmond reported on the irregularities she encountered while trying to retabulate out of balance precincts. She indicated that in some cases staff could not retabulate because the number of physical ballots counted in the container did not match the number of voters according to the poll book. Staff also requested the applications to vote for Detroit precinct 444 and precinct 262. Both containers ha[d] fewer ballots in the container than the number of voters according to the poll book, but what was strange was there appeared to be some missing applications." 4.
7. It was reported that in the August 2020 primary that 72% of Detroit's absentee voting precincts were out of balance.
8. After discussion among the Board members, I voted along with all the other canvassers in a unanimous vote in favor of certifying the August 4, 2020 Primary Election.

9. Although certifying the primary election results, all Board members expressed serious concerns about the irregularities and inaccuracies. The Board unanimously approved a proposed joint resolution titled "Requesting a State Election Monitor and Investigation" that stated "Now Therefore Be it Resolved That, The Board of Canvassers for the County of Wayne, Michigan, request for the Secretary of State as Michigan's Chief Election Officer, to appoint a monitor to supervise the training and administration of the City of Detroit, Absentee Voter Counting Boards in the 2020 November General Election. Be it Finally Resolved, That, the Board of Canvassers for the County of Wayne, Michigan, request an investigation be conducted by the State Department of Elections into the training and processes used by the City of Detroit in the 2020 August Primary Election."

10. On November 3, 2020, the general election was held. I went to observe the election process at the TCF Center on November 3, 2020 and November 4, 2020.

11. Since November 5, I went to the Wayne County Canvas almost every day and helped the Wayne County staff.

12. On November 17, 2020, there was a board of Canvassers meeting scheduled to start at 3:00pm to determine whether or not to certify the November election. The meeting did not begin until 4:46pm.

13. Minutes before the meeting began at 4:46pm, I was given a report on the final canvas. We were not given an executive summary which was customary at most other certification meetings.

14. During this meeting, I determined that more than 70% of Detroit's 134 Absent Voter Counting Boards (AVCB) did not balance and many had no explanation to why they did not balance.

15. Vice-Chair Kinloch made a motion to certify the vote. I noted our prior reservations about unbalanced precincts in August 2020 and determined the record had discrepancies and irregularities and was incomplete.

16. A motion was made to certify the vote, and I voted not to certify. The vote to certify the Wayne County elections failed 2-2.

17. After the vote, my Democrat colleagues chided me and Mr. Hartmann for voting to not certify.

18. After the vote, public comment period began and dozens of people made personal remarks against me and Mr. Hartmann. The comments made accusations of racism and threatened me and members of my family. The public comment continued for over two hours and I felt pressured to continue the meeting without break.

19. After several hours of harsh comments, Vice-Chair Kinloch suggested a potential resolution. Wayne County Corporate Counsel Janet Anderson-Davis told me that I had to certify the vote that night. She told the members their role was ministerial and they could not use their discretion on matters like the record being incomplete. We were told that discretion was outside the board's authority.

20. After being told by Ms. Anderson-Davis that I could not use my discretion regarding the anomalies, I believed I had no choice but to certify the results despite my desire to oppose certification based on the incomplete record.

21. Additionally, we were presented with a resolution that promised a full, independent audit that would present answers to the incomplete record. I voted to agree to certify based on the promise of a full, independent audit. I would not have agreed to vote to certify but for that promise of a full, independent audit.

22. Vice-Chairman Jonathan Kinloch gave me assurances that voting for the certification of the November election would result in a full, independent audit of Detroit's unbalanced precincts. I relied on that assurance and voted to certify the election based on that assurance. Without that assurance I would not have voted to certify the Wayne County November election.

23. Later that evening, I was sent statements that Secretary Jocelyn Benson made saying that she did not view our audit resolution to be binding. Her comments disputed the representations made by Vice-Chair Kinloch on which I relied.

24. As a result of these facts, I rescind my prior vote to certify Wayne County elections.

25. I fully believe the Wayne County vote should not be certified.

26. The Wayne County election had serious process flaws which deserve investigation. I continue to ask for information to assure Wayne County voters that these elections were conducted fairly and accurately. Despite repeated requests, I have not received the requisite information and believe an additional 10 days of canvas by the State Board of Canvassers will help provide the information necessary.

27. I initially voted not to certify the election, and I still believe this vote should *not* be certified and the State Board of Canvassers should canvass for an additional period.

28. Until these questions are addressed, I remain opposed to certification of the Wayne County results.

The above information is true to the best of my information, knowledge, and belief.

I certify under penalty of perjury, that my statement and the evidence submitted with it, are all true and correct.

Printed Name: Monica S Palmer

Signed Name: Monica S Palmer

Date:

Sworn to before me this 18 day of November 2020 at 9:33 pm

My Commission expires on: 08/3/2022

JANICE L. DANIELS
NOTARY PUBLIC - STATE OF MICHIGAN
COUNTY OF OAKLAND
My Commission Expires August 3, 2022
Acting in the County of WAYNE

EXHIBIT 14

Affidavit of Lisa Gage (Dec. 10, 2020)

AFFIDAVIT OF LISA GAGE

Lisa Gage, being sworn, declares under penalty of perjury:

1. I am personally familiar with the facts stated in this Affidavit and, if sworn as a witness, am competent to testify to them as well.

2. I am a registered voter in the State of Michigan.

3. I was a Republican Poll Challenger on November 3, and November 4, 2020.

4. On November 3, 2020 I was observing at TCF Center in Detroit Michigan.

5. I began observing the processing and counting of absentee ballots at 7:00 am on November 3, 2020. There were approximately 140 tables with five poll workers at each table.

6. I observed several irregularities with the 20-30 tables I was able to spend time observing in detail.

7. I was not assigned to a specific precinct. The first precinct table I observed only had 10 ballots. I then moved on to another table with no GOP Challenger present.

8. Generally, the process I observed, was that the person that was at the e-poll computer would first scan the bar code on the envelope with a hand-held scanner. The voter's name, date of birth, and registration status would appear on a computer monitor on the table. If the voter's name did not appear on the computer monitor, poll workers were supposed to type in the voter's name, and if the name did not appear, check for the voter's name on an Absentee Voter List ("AV List"). The AV List would include voters who registered and voted on Monday and Tuesday, election day.

9. After checking that information, the envelope was to be passed to another person who separated the envelope from the secrecy envelope that contained the ballot.

10. The next person would take the ballot out of the secrecy envelope and pass the ballot to the next worker who would roll it to flatten it, tear off the perforated stub with the ballot number, and then put the ballot into a box identified as the "tabulation box" with other processed ballots that was then taken to a tabulator when the box had up to 50 ballots. I would estimate that I saw thousands of ballots placed in the tabulation box during the time I worked at the TCF.

11. There was no signature comparison being conducted on absentee ballots. There were stacks of ballots in "post office" bins in their envelopes, on tables identified by precinct number.

12. Between 9:00 and 9:30 am, I asked a supervisor about signature comparison for the ballots currently on the table. She was a slightly overweight, African-American woman with shoulder length hair. She wore one of the white shirts with an election insignia on the shirt. As with all other election workers, she did not have a name tag. This supervisor told me "that was done somewhere else".

13. A poll worker said "we have 10 ballots, just like yesterday (meaning Monday)". When I heard this, I approached a supervisor because I thought it was unusual that there would be just 10 on one day and then just 10 the next day. The supervisor told me that they had ballots on Tuesday that they had "partially processed on Monday." This supervisor wore a white shirt with election insignia and no name tag, but was a

different supervisor identified in paragraph 11. With these repeat ballots, the poll workers followed the 5 step process outlined above.

14. Later that morning approximately between 11:45am and 12:30pm, a third supervisor announced that they "needed to catch up". This supervisor was tall, approximately 5'9" average build, late 40', early 50-ish, short hair, African-American woman. She also wore the white shirt with election insignia with no name tag. At this point the ballots were just divided up between each of the poll worker at the table who opened envelopes, pulled the stub and put the ballots in the tabulator box. The entire 5 step process was entirely abandoned. There was no scanning of the outside of the envelope to check for registration status, there was no signature, or ballot number verification.

15. There was no post mark verification ; there was no ballot review for stray marks; there was no verification of the voter existing in the data base; there was no signature comparison or authentication.

16. I estimate that thousands ballots were processed this way.

17. None of the outer envelopes that I observed, included any additional written statements or stamps in addition to the signature, and if there had been I would have noticed them. I estimate these outer envelopes that I was able to see to be at least several hundred to a thousand.

18. These non-verified ballots were then placed in a box and then a separate worker took the box to the tabulator, without any review.

19. As a challenger I was prohibited from observing the postmarks. I was told many times by a supervisor that I had to "stand away".

20. As a challenger I was prohibited from observing the ballot duplication process by poll workers moving in front of me to block me from watching the duplication process. Poll works are supposed to have three people involved in the duplication process: a Democrat, a Republican, and an independent observing the process. One of the three would mark the duplicate ballot, while another person called out the selections.

21. Once the duplicate was made, the poll workers deposited the original into an envelope, marked 'Originals'. As poll challengers were not able to see what happened to the envelope. I asked a Supervisor as to the disposition of the originals, and was told the originals envelope will stay in the supplies box. Having observed other challengers being escorted out of the site, and the noticeable disgust at my asking questions, I felt that too much inquiry could result into dismissal from the site.

22. Over the course of the day, I changed my tactic and would ask a variety of supervisors a question instead of multiple questions to any one or two supervisors. I left the TCF Center on November 3, 2020 mid-afternoon as it appeared no more ballots were coming in. Contributing to my decision to leave was that GOP challengers were denied the ability to sit in unoccupied chairs by either poll workers or supervisors. We were not allowed to pull chairs away from the table; we were not permitted to leave to get food and were told by republican resources that if we left we would not be able to return. Other GOP challengers and myself observed Democrat challengers sit at the tables with the poll workers. We were not even permitted to place a water bottle on an unused corner of the tables. We were left to juggle water bottles pens, note papers and other documents, making note taking difficult.

23. On November 4, 2020, I returned to TCF at 6:30am.

24. I returned to the same general area I had been on the day before. I started observing four tables but eventually observed many different tables.

25. I observed incomplete and inconsistent E-poll documentation, table to table.

26. The E-poll system allowed ballot acceptance even when date of birth and/or voter registration dates were suspect. For example, I observed a voter date of birth 20 years AFTER the date of voter registration. The poll worker simply processed the ballot without inquiry. I tried to challenge this ballot and was told that the ballot would go into the "problem bin". The "problem bin" was at the table. At various times the "problem bin" would be taken the "bull pen" or in some cases, directly to the tabulation area.

27. On one occasion I witnessed two of the ballots that I challenged, being fed through the tabulator without adjudication. The poll worker that processed this ballot saw me watching this process and stared back at me with indignation.

28. I specifically observed 26 ballots that were not verified with either e-poll or the AV list. This list of 26 is attached. I attempted to challenge these 26 ballots, although the poll workers would not acknowledge my challenges. The 26 ballots on this list were observed by me in the span of a few hours. There were other ballots that I could have challenged for the same reasons, but these 26 were the ones that I was able to write down as the pace of processing increased. The 26 were observed in a couple of hours at a single table on Wednesday November 4. There were over 140 tables in the counting room.

29. Each of the ballots on the list of 26 I challenged were tabulated without adjudication. It can be observed that these ballots were sequential, highly suggestive of fraud, due to the fact that each clerk must assign a ballot number as the applications for absent voter ballots arrive in the clerk's office. The chance of the same ballots being applied for and then returned for tabulation as the same time is remote.

30. When the military ballots came in, I observed, all were in the E-poll system. However there were inconsistencies between dates of birth and voter registration on the vast majority of the ballots I observed. For example, I observed an active duty ballot, with a voter date of birth of 1938, with a voter registration date of 2020.

31. I made a point to examine every military ballot for date of birth and date of voter registration. A vast majority contained dates of birth between 1938 and 1960 for active duty ballots. They had e-poll addresses of Detroit, MI, rather than a deployment location. Also there were only a handful of "voting locations" identified in the e-poll for approximately 100 ballots. I noticed that these same "voting locations" would come up again and again as these military ballots were being processed. I would estimate this to be approximately 100 ballots at the multiple tables I was observing. There were approximately 143 tables.

32. Of all the military ballots I observed, none were in AV envelopes. There were less than 5 in larger manila envelopes, the rest were in standard white business envelopes.

33. I observed the opening of military ballots that arrived in standard white business envelopes. I did not see any voter signature certificates come out of these envelopes as required by law.

34. I observed the duplication process of the each of the military ballots onto the machine readable ballot forms. The original, 8/5x11 papers were put back in their mailing envelopes and placed in the originals envelope.

35. During a time when there was no activity, I observed that the system clock time on the screen saver on the E-poll system monitors varied by up to 5 hours, thereby rendering inability to verify date and time stamp for data verification later. This would make it easy for ballots to be excluded if a review was time specific.

36. I also experienced attempts at intimidation. When I began challenging ballots I was approached by individuals identifying as from the NAACP or a "civil rights group" accusing me of acting in "bad faith"; telling me that I was violating "civil rights" by challenging ballots.

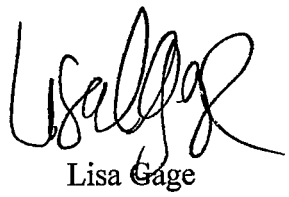
37. I was able to resist the intimidation but I did observe other Republican poll challengers become visibly upset by this activity. I was asked to replaced several poll challengers who had become rattled. I observed a Republican poll challenger arrested for taking off his mask when he experienced breathing problems. The poll workers would cheer and clap whenever a Republican poll challenged was escorted out.

38. I was also approached by an "activists" who inserted himself into a particular challenge discussion, offering his opinion that my challenge was in bad faith. He later identified himself as a University of Michigan Law School student, stating he and others decided to come to TCF to be involved.

39. Once the actual attorneys were present, these activists moved on.

40. Other forms of intimidation were body blocking, deprivation of chairs to sit in. Then when Republican poll challengers left to get food or drink, they were denied re-entry.

41. Dated: December 10, 2020



Lisa Gage

Subscribed and sworn to before me on:

/s/ Sarah Elwood

Notary public, State of Michigan, County of: Ionia

My commission expires: 5/16/21

EXHIBIT 15

Affidavit of Ben Cotton (Apr. 8, 2021)

STATE OF MICHIGAN

IN THE CIRCUIT COURT FOR THE COUNTY OF ANTRIM

WILLIAM BAILEY

Plaintiff

Case No. 20-9238-CZ

v.

ANTRIM COUNTY

HON. KEVIN A. ELSENHEIMER

Defendant,

SECRETARY OF STATE JOCELYN BENSON

Intervenor-Defendant,

Matthew S. DePerno (P52622)
DEPERNO LAW OFFICE, PLLC
Attorney for Plaintiff
951 W. Milham Avenue
PO Box 1595
Portage, MI 49081
(269) 321-5064

Haider A. Kazim (P66146)
CUMMINGS, MCCLOREY, DAVIS & ACHO, PLC
Attorney for Defendant
319 West Front Street
Suite 221
Traverse City, MI 49684
(231) 922-1888

Heather S. Meingast (P55439)
Erik A. Grill (P64713)
Assistant Attorneys General
Attorneys for Proposed Intervenor-Defendant Benson
PO Box 30736
Lansing, MI 48909
(517) 335-7659

AFFIDAVIT OF BENJAMIN R. COTTON 8 APRIL 2021

I, Ben Cotton, being duly sworn, hereby depose and state as follows:

1) I am over the age of 18, and I understand and believe in the obligations of an oath. I make this affidavit of my own free will and based on first-hand information and my own personal observations.

2) I am the founder of CyFIR, LLC (CyFIR).

3) I have a master's degree in Information Technology Management from the University of Maryland University College. I have numerous technical certifications, including the Certified Information Systems Security Professional (CISSP), Microsoft Certified Professional (MCP), Network+, and Certified CyFIR Forensics and Incident Response Examiner.

4) I have over twenty five (25) years of experience performing computer forensics and other digital systems analysis.

5) I have over eighteen (18) years of experience as an instructor of computer forensics and incident response. This experience includes thirteen (13) years of experience teaching students on the Guidance Software (now OpenText) EnCase Investigator and EnCase Enterprise software.

6) I have testified as an expert witness in state and federal courts and before the United States Congress.

7) I regularly lead engagements involving digital forensics for law firms, corporations, and government agencies.

8) In connection with this legal action I have had the opportunity to examine the following devices:

a) Antrim County Election Management Server Image. This image was acquired on 4 December 2020 by a firm named Sullivan and Strickler.

b) Thirty eight (38) forensic images of the compact flash cards used in Antrim County during the November 2020 elections that were imaged on 4 December 2020 by a firm named Sullivan and Strickler.

c) One (1) SID-15v-Z37-A1R, commonly known as the Image Cast X (ICX), that was used in the November 2020 elections

d) Two (2) Thumbdrives that were configured for a precinct using the ES&S DS400 tabulator that were used during the November 2020 election.

e) One ES&S server that was used in the November 2020 election.

9) **Internet Communications with the Dominion ICX.** I examined the forensic image of a Dominion ICX system utilized in the November 2020 election and discovered evidence of internet communications to a number of public and private IP addresses. Of specific concern was the presence of the IP address 120.125.201.101 in the unallocated space of the 10th partition of the device. This IP address resolves back to the Ministry of Education Computer Center, 12F, No 106, Sec.2,Hoping E. Rd.,Taipei Taiwan 106. This IP address is contextually in close proximity to data that would indicate that it was part of the socket configuration and stream of an TCP/IP communication session. Located at physical sector 958273, cluster 106264, sector offset 256, file offset 54407424 of the storage drive, the unallocated nature of the artifact precludes the exact definition of the date and time that this data was created. Also located in close proximity to the Ministry of Education IP address is the IP address 62.146.7.79. This IP address resolves to a cloud provider in Germany.

Figure 1-IP Addresses Located in Unallocated Space

Further examination of the ICX clearly indicates that this system is also actively configured to communicate on a private network of 10.114.192.x with FTP settings to connect to 10.114.192.12 and 10.114.192.25. Also apparent is that at one time this system was configured to have the IP address 192.168.1.50. This IP address is also a private IP range. These IP configurations and artifacts definitively identify two things, 1) the device has been actively used for network communications and 2) that this device has communicated to public IP addresses not located in the United States. Further analysis and additional devices would be required to determine the timeframe of these public IP communications.

10) **<u>ESS DS400 Communications.</u>** A careful examination of the ESS DS400 devices and thumb drives was conducted. This examination proved that each DS400 had a Verizon cellular wireless communications card installed and that the card was active on powerup, which meant that there is the ability to connect to the public internet on these devices as well. Both of the DS400 devices were configured to transmit election results to IP address 10.48.51.1. This is a private network, which means that it would only be accessible by the remote DS400 systems through leveraging the public internet and establishing a link to a communications gateway using a public IP or via a virtual private network (VPN). It is important to understand that this

communication can only occur if the cellular modems have access to the public internet. I did not have the entire communications infrastructure for the private network and given this lack of device production associated with the DS200, I can not say which other devices may have connected to this private network nor the full extent of the communications of nor the remote accesses to the DS400 devices.

11) **Out of Date Security Updates and Virus Definitions.** An analysis of operating system, and antivirus settings on the servers and computers provided to me was conducted. It was immediately apparent that these systems were extremely vulnerable to unauthorized remote access and manipulation. For example, none of the operating systems had been patched nor the antivirus definition files updated for years. The Antrim EMS was last updated in 2016. The other systems were in a similar state. This lack of security updating has left these systems in an extremely vulnerable state to remote manipulation and hacking. Since 2016 more than ninety seven (97) critical updates have been issued for the Windows 10 operating system to prevent unauthorized access and hacking. The fact that these systems are in such a state of vulnerability, coupled with the obvious public and private internet access, calls the integrity of the voting systems into question. The Halderman report dated March 26, 2021 relating to this matter validates this finding. It also validates that the system is in a state such that an unauthorized user can easily bypass the passwords for the system and database to achieve unfettered access to the voting system in a matter of minutes. These manipulations and password bypass methodologies can be performed remotely if the unauthorized user gains access to the system through the private network or the public internet.

12) **Incomplete Compliance with the Subpoena for Digital Discovery.** Antrim County has apparently failed to produce all of the voting equipment for digital preservation and analysis. I

examined the purchase documents produced by Antrim County with respect to the purchase of the Dominion Voting system and note that the following system components listed on the purchase documents were not produced:

(a) ImageCast Listener Express Server

(b) ImageCast Express Firewall

(c) EMS Express Managed Switch

(d) ICP Wireless Modems (17)

(e) Image Cast Communications Manager Server

(f) ImageCast Listener Express RAS (remote access server) System

(g) ImageCast USB Modems (5)

Without these system components it will be impossible to determine the extent of public and private communications, the extent to which remote access to the voting system components is possible and to determine if or when unauthorized access occurred.

SIGNED UNDER THE PAINS AND PENALTIES OF PERJURY THIS 8th DAY OF April 2021.

Benjamin R. Cotton

EXHIBIT 16

Letter, Rep. Francis X. Ryan, Pennsylvania House of Representatives, to Rep. Scott Perry, U.S. House of Representatives (Dec. 4, 2020)

December 4, 2020

Congressman Scott Perry
1207 Longworth House Office
Building Washington, DC 20515

Congressman Perry;

The general election of 2020 in Pennsylvania was fraught with inconsistencies, documented irregularities and improprieties associated with mail-in balloting, pre-canvassing, and canvassing that the reliability of the mail-in votes in the Commonwealth of Pennsylvania is impossible to rely upon.

The above factors, when combined with the lack of the required associated internal control mechanisms to ensure legality, accountability, accuracy, and the trustworthiness of the results, effectively undermine the trustworthiness of the entire election process.

The House of Representatives of Pennsylvania determined, as a result, that the process by which the President of the United States was determined was so fraught with errors that the legislature introduced House Resolutions 1094 on November 30, 2020 to contest the selection of electors.

The analysis below substantially confirms that the mail-in ballot process in the Commonwealth of Pennsylvania in the 2020 General Election was so defective that it is essential to declare the selection of presidential electors for the Commonwealth to be in dispute. The United States Congress is asked to declare the selection of presidential electors in this Commonwealth to be in dispute and to intervene in the selection of the electors for the Commonwealth of Pennsylvania for the 2020 General Election.

In any process control environment, the system of internal controls is designed to reasonably deter wrongdoing.

In the Sarbanes-Oxley type environment and the Committee on Sponsoring organizations process control environment, the control environment surrounding an election require that the processes utilized be capable of providing reasonable controls to ensure that the election results reflect the will of the voters.

In that regard, the COSO standards (Committee on Sponsoring Organizations) prescribes processes of controls to ensure internal controls are adhered to, for instance, in this case, the accuracy of the election results. COSO and SOX are built on the same model of the system of internal controls

The control environment includes:

1. ***Control Environment***

- Exercise integrity and ethical values.
- Make a commitment to competence.
- Use the board of directors and audit committee.
- Facilitate management's philosophy and operating style.
- Create organizational structure.
- Issue assignment of authority and responsibility.
- Utilize human resources policies and procedures.

2. ***Risk Assessment***

- Create companywide objectives.
- Incorporate process-level objectives.
- Perform risk identification and analysis.
- Manage change.

3. ***Control Activities***

- Follow policies and procedures.
- Improve security (application and network).
- Conduct application change management.
- Plan business continuity/backups.
- Perform outsourcing.

4. ***Information and Communication***

- Measure quality of information.
- Measure effectiveness of communication.

5. ***Monitoring***

- Perform ongoing monitoring.
- Conduct separate evaluations.

In any system of internal controls, there are audits which would identify control deficiencies, significant deficiencies, and material weaknesses of the system of internal controls. When there are such deficiencies of internal controls of the material weakness nature and/or significant deficiency nature than standards require that the results cannot be relied upon. The accounting

profession has specific guidance on such control environment in AU-314, Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement.

In 2019, Rep. Ryan identified such concerns about the control environment in the Commonwealth and introduced House Bill 1053, Lean Government Operations, to uniformly implement lean operations and an effective system of internal controls. The Governor indicated opposition to the bill and threatened to veto the bill. In the State Government Committee the bill passed 20-5 when the Democrat members placed such significant amendments and opposition from the executive branch to preclude the bill from moving.

This pattern of obstruction to systems of internal controls reinforces the concerns that the control environment did not exist in Pennsylvania's executive branch to warrant confidence that there was any intent to establish an effective system of internal controls over the mail-in ballots in the Commonwealth.

In 2019, we identified such concerns about the control environment in the Commonwealth were identified and a bill to address these concerns was introduced. and introduced House Bill 1053 was introduced to uniformly implement lean government operations in order to uniformly implement lean operations and an effective system of internal controls. The Governor indicated opposition to the bill and threatened to veto the bill. Additionally, Democrat members in the House State Government Committee cited the Governor's opposition to the bill as they sought to defeat the bill through the amendment process. In the State Government Committee the bill passed 20-5 when the Democrat members placed such significant amendments and opposition from the executive branch to preclude the bill from moving.

This pattern of obstruction to systems of internal controls reinforces the concerns that the control environment did not exist in Pennsylvania's executive branch to warrant confidence that there was any intent to establish an effective system of internal controls over the mail-in ballots in the Commonwealth.

In any audit committee the Audit Committee and with auditing standards, the question is always asked in the management representation letters: "Was management (read Executive Branch) able to override the system of internal controls?" Should the answer to that question be YES, which in the instant case, it was, the CPA audit would immediately stop with NO audit opinion issued. Nothing less can should be expected of our election process.

For the reasons below, it is believed that the system of controls over voting within the Commonwealth of Pennsylvania in the 2020 General Election were so flawed as to render the results of the mail-in ballot process incapable of being relied upon. Specific potential remedies are available to include:

1. Revote of the mail in ballots in time to certify the electors for the presidential election.
2. Declare the process of mail in ballots so flawed that the Congress of the United States, as prescribed by the U. S. Constitution would select the PA electors for President.

The evidence of resistance to the implementation to election security safeguards, process flaws, inconsistencies, violations of PA election laws as written, include:

1. Documented objection by leaders of the Democrat Party to object to a study of the election process to preclude the problems that in fact did occur in the 2020 general election. The study was proposed as House Resolution 1032 of 2020 and was abandoned after gross public misrepresentations were made about the true nature of the intent of the resolution. due to public backlash due to the comments (An example of this can be found in the comments of Representative Malcolm Kenyatta.)
2. Actions from the PA Supreme Court which undermined the controls inherent in Act 77 of 2019. The "legislative" overreach by the Supreme Court is the basis of the impeachment articles against Justice Wecht. The controls which were undermined include:
    a. On September 17, 2020, less than seven weeks before the November 3, 2020 election, the partisan majority on the Supreme Court of the Commonwealth of Pennsylvania unlawfully and unilaterally extended the deadline for mail-in ballots to be received, mandated that ballots mailed without a postmark would be presumed to be received timely, and could be accepted without a verified voter signature.
    b. On October 23, 2020, less than two weeks before the November 3, 2020 election and upon a petition from the Secretary of the Commonwealth, the Supreme Court of the Commonwealth of Pennsylvania ruled that mail-in ballots need not authenticate signatures for mail-in ballots, thereby treating in-person and mail-in voters dissimilarly and eliminating a critical safeguard against potential election crime.
    c. Authorized the use of drop boxes for collecting votes with little to no controls proscribed to prevent ballot harvesting.
3. Actions by the Secretary of State which undermined the consistency and controls of the election process during the weeks preceding the General Election of November 3, 2020. The actions by the Secretary led to a House Resolution to prohibit object to the seating of electors calling the election to be in dispute. These include:
    a. On November 2, 2020, the night before the November 3, 2020 election and prior to the prescribed time for pre-canvassing mail-in ballots, the office of the Secretary of the Commonwealth encouraged certain counties to notify party and candidate representatives of mail-in voters whose ballots contained defects;
    b. Heavily Democrat counties permitted mail-in voters to cure ballot defects while heavily Republican counties followed the law and invalidated defective ballots;
    c. In certain counties in the Commonwealth, watchers were not allowed to meaningfully observe the pre-canvassing and canvassing activities relating to absentee and mail-in ballots;
    d. In other parts of the Commonwealth, watchers observed irregularities concerning the pre-canvassing and canvassing of absentee and mail-in ballots.
4. Prior attempts to cure the problems associated with Act 77 of 2019, the election Reform Code where incorporated into House Bill 2626 of the 2019-2020 session. The Governor threatened to veto the bill when it became apparent that the Supreme Court was going to incorporate more favorable changes to Act 77 of 2019 than House Bill 2626 authorized.

5. Permitted inconsistent drop box processes by counties with little to no controls or audits processes which essentially gave way to substantial opportunities for ballot harvesting.
6. The Secretary of State has shown bias in get-out-the-vote efforts due to the Secretary's coordination efforts for get out the vote efforts only in Democrat party-controlled counties and localities.

In addition to the concerns of the actions of the Secretary of State and the legislative overreach by the Pennsylvania Supreme Court, the inaccuracies of the actual results themselves call into question the accuracy of the SURE system, the consistency of the application of voting laws throughout the counties. Certain inconsistencies stand out to include:

At the county level the pattern of inconsistencies is easily seen. For instance, Over-vote in Philadelphia County -- On November 4th at 11:30am, the DOS posted updated mail in vote counts for Philadelphia County. The number of ballots reported to have been counted was an impossible 508,112 ballots despite the fact that only 432,873 ballots had been issued to voters in that county. Later that day, the ballots counted number was reduced but this begs the question, who had the authority to add and subtract votes on the ballot counts reported to the Department of State? Even if this was simply a data entry error, the lack of internal controls over such reporting necessitates a review of the numbers, the process and system access.

Information Sharing -- Members of the legislature or any oversight body of election inspectors, were not provided access to any data that was not available to the general public in open source records. There are many other anomalies that one could not include in the letter because we have not been provided with the information you need to evaluate. We have had to file right to know Right-to-Know requests to access the data. Whenever the systems lack transparency it is IMPOSSIBLE for anyone to contend that fraud did not occur.

Mail Date

- Ballots Mailed on or BEFORE 9-11-2020. That total is 27995.
- Ballots Mailed on November 1, 2 or 3. That total is 8163.
- Ballots with NO MAILED date. That total is 9005.
- Ballots Returned on or BEFORE the Mailed Date. That total is 58221.
- Ballots Returned one day after Mailed Date. That total is 51200.

Voter Date of Birth

- Mail Votes cast by voters over the age of 100. That total is 1532.
- In Allegheny County, there were 41 ballots mailed to people born on 01/01/1800- making them all 220 years old.
- Mail Votes by voters with NO Date of Birth. That total is 245.

Additionally, in a data file received on November 4, 2020, the Commonwealth's PA Open Data sites reported over 3.1 million mail in ballots sent out. The CSV file from the state on November 4 depicts 3.1 million mail in ballots sent out but on November 2, the information was provided

that only 2.7 million ballots had been sent out. This discrepancy of approximately 400,000 ballots from November 2 to November 4 has not been explained.

This apparent discrepancy can only be evaluated by reviewing all transaction logs into the SURE system to determine the access, authority for the entry, the verification of the data entered as well as the authentication of the security certificates of the sites from which the data had been entered.

It is also important to note that the Department of State removed all election data from the PA Open Data platform in Mid-November 2020. They provided no explanation for removing the data. That is part of the issue—the data changed over time despite the fact that the number of ballots mailed should not have changed after November 2nd and the number of mail ballots received/cast should not have changed after November 3rd.

In light of the above, the mail-in ballot process in the Commonwealth of Pennsylvania in the 2020 General Election was so defective that it is essential to declare the selection of presidential electors for the Commonwealth to be in dispute. The United States Congress is asked to declare the selection of presidential electors in this Commonwealth to be in dispute and to intervene in the selection of the electors for the Commonwealth of Pennsylvania for the 2020 General Election.

Respectfully Submitted,

Francis X. Ryan, Member
101st Legislative District, PA

Brad Roae, Member
6th Legislative District, PA

Daryl Metcalfe, Member
12th Legislative District, PA

Mike Puskaric, Member
39th Legislative District, PA

Valerie Gaydos, Member
44th Legislative District, PA

Eric Nelson, Member
57th Legislative District, PA

Kathy L. Rapp, Member
65th Legislative District

Stephanie Borowicz, Member
76th Legislative District, PA

David Rowe, Member
85th Legislative District, PA

Rob Kauffman, Member
89th Legislative District, PA

Mike Jones, Member
93rd Legislative District, PA

David Zimmerman, Member
99th Legislative District, PA

Jim Cox, Member
129th Legislative District, PA

Barbara Gleim, Member
199th Legislative District, PA

Russ Diamond, Member
102nd Legislative District

Cc: Members of the United States House of Representatives, Members of the United States Senate, President of the United States, Governor Tom Wolf, Secretary State of Pennsylvania, PA Senator Jake Corman, PA Senator Kim Ward, PA Speaker of the House Bryan Cutler, and PA Representative Kerry Benninghoff

EXHIBIT 17

Wisconsin Legislative Audit Bureau Report (Oct. 2021)

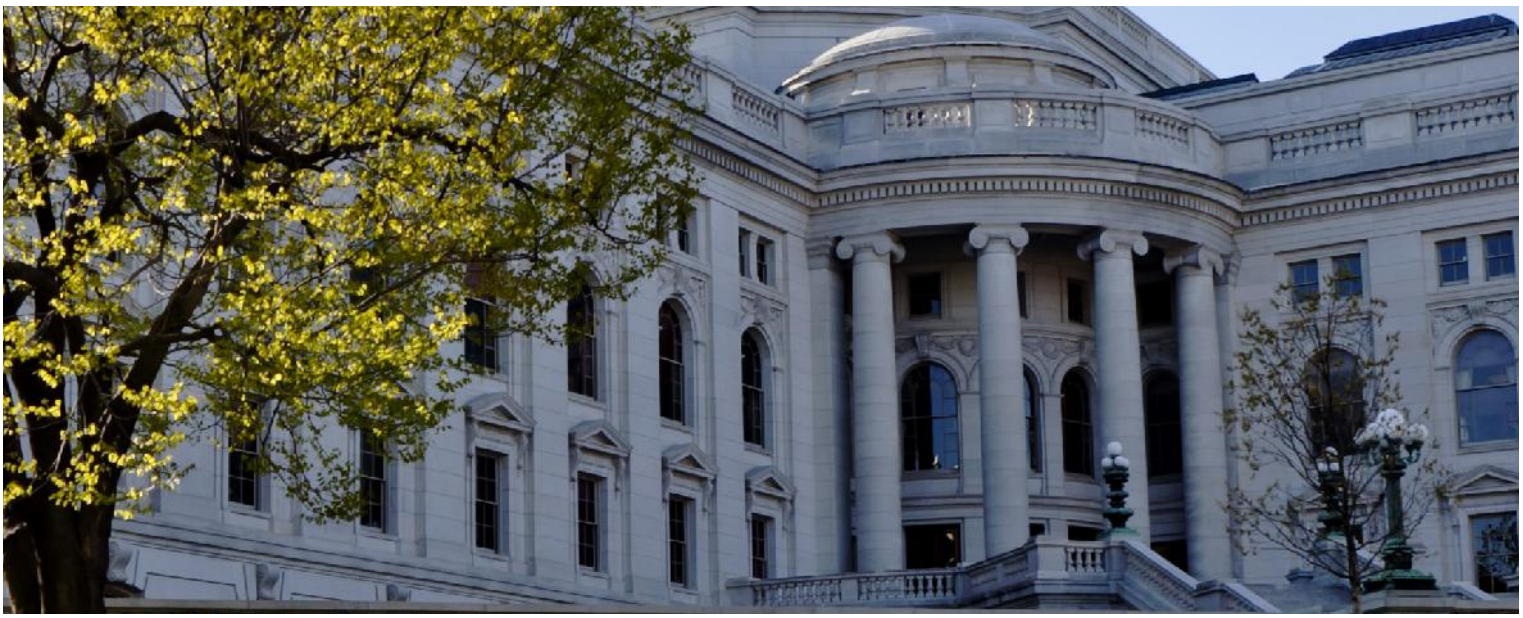
STATE OF WISCONSIN

Legislative Audit Bureau

NONPARTISAN • INDEPENDENT • ACCURATE

Report 21-19
October 2021

Elections Administration



Joint Legislative Audit Committee Members

Senate Members:

Robert Cowles, Co-chairperson
Dale Kooyenga
Howard Marklein
Melissa Agard
Tim Carpenter

Assembly Members:

Samantha Kerkman, Co-chairperson
John Macco
Mark Born
Dianne Hesselbein
Francesca Hong

Elections Administration

STATE OF WISCONSIN

Legislative Audit Bureau

NONPARTISAN • INDEPENDENT • ACCURATE

Report 21-19
October 2021

Report 21-19
October 2021

Legislative Audit Bureau

State Auditor
Joe Chrisman

Deputy State Auditor for Performance Evaluation
Dean Swenson

Team Leaders
Nehemiah Chinavare
Ross Ryan
Maria Toniolo

Evaluators
Jacob Dominy
Grace Herndon
John Holland
Anne Lombardi
James Malone
Andrew McGuire
Madeline McIlhon
Sam Rebenstorf
Jonathan Sandoval
Erik Thulien
Addison Tryon
Kendall Vega
Charlie Warzecha

Publications Designer and Editor
Susan Skowronski

The Legislative Audit Bureau supports the Legislature in its oversight of Wisconsin government and its promotion of efficient and effective state operations by providing nonpartisan, independent, accurate, and timely audits and evaluations of public finances and the management of public programs. Bureau reports typically contain reviews of financial transactions, analyses of agency performance or public policy issues, conclusions regarding the causes of problems found, and recommendations for improvement.

Reports are submitted to the Joint Legislative Audit Committee and made available to other committees of the Legislature and to the public. The Audit Committee may arrange public hearings on the issues identified in a report and may introduce legislation in response to the audit recommendations. However, the findings, conclusions, and recommendations in the report are those of the Legislative Audit Bureau.

The Bureau accepts confidential tips about fraud, waste, and mismanagement in any Wisconsin state agency or program through its hotline at 1-877-FRAUD-17.

For more information, visit *www.legis.wisconsin.gov/lab*.

Contact the Bureau at 22 East Mifflin Street, Suite 500, Madison, Wisconsin 53703; *AskLAB@legis.wisconsin.gov;* or (608) 266-2818.

Contents

Letter of Transmittal **1**

Introduction **3**

Training **9**

Municipal Clerks 9
Compliance with Training Requirements 11
Issues for Legislative Consideration 13
Satisfaction Levels of Clerks 13
Other Local Election Officials 16
Chief Election Inspectors 16
Other Election Officials 16

Maintenance of Voter Registration Records **19**

Voter Registration 19
Personally Identifiable Information 20
Data Agreement 23
Issue for Legislative Consideration 24
Duplicate Voter Registration Records 25
Deceased Individuals 26
Data Agreement 28
Individuals Serving Felony Sentences 28
Data Agreement 30
Post-Election Review 31
Electronic Registration Information Center (ERIC) 31
Issue for Legislative Consideration 34
Satisfaction Levels of Clerks 35

Absentee Ballots **37**

Voting by Absentee Ballot 37
November 2020 General Election 38
Absentee Ballot Certificates 40
Review of Certificates 42
Election Day Forms 44
Improved Procedures 44
Issues for Legislative Consideration 45
Collection of Absentee Ballots 46
Drop Boxes 46
Special Events 48
Issue for Legislative Consideration 49
Indefinitely Confined Individuals 49
Special Voting Deputies 52
Improved Procedures 53
Issue for Legislative Consideration 54

Ballot Processing **55**

Central Count Locations 55
Election Day Forms 56
Ballot Security 57
Poll Workers 58
Issue for Legislative Consideration 60
Ballot Counting 61
Polling Places 62
Issue for Legislative Consideration 63
Reconciliation Process 63

Electronic Voting Equipment **67**

Equipment Approval 67
Types of Equipment Used 68
Issue for Legislative Consideration 70
Equipment Integrity 71
Pre-Election Tests 71
Tamper-Evident Seals 73
Issue for Legislative Consideration 75
Satisfaction Levels of Clerks 75
Administrative Rule Promulgation 77

Post-Election Audit **79**

Post-Election Audit Procedures 79
Post-Election Audit Results 80
Equipment Error Rate 83
Post-Election Audits in Other States 84
Issues for Legislative Consideration 85

Complaints Filed with Clerks **87**

Number of Complaints 87
Clerk Actions 89

Complaints and Concerns Filed with WEC **93**

Number of Complaints 93
Complaint Resolution 94
Concerns 97
Improving Procedures 98
Issue for Legislative Consideration 100

Election Recount Costs **101**

Estimated Recount Costs 102
Actual Recount Costs 104
Staffing 106
Facilities 107
Election Systems and Equipment 109
Issues for Legislative Consideration 109

Appendices

Appendix 1—WEC Commissioners, by Appointing Authority

Appendix 2—Eight Groups Involved with Elections Administration Issues That We Contacted

Appendix 3—Municipal Clerks and County Clerks That We Contacted, by County

Appendix 4—Review of a Sample of Absentee Ballot Certificates in the November 2020 General Election

Appendix 5—319 Municipalities for Which We Reviewed Election Day Forms, by County

Appendix 6—Review of a Sample of Electronic Voting Equipment Test Results

Appendix 7—Report Recommendations, by Chapter

Appendix 8—Legislative Considerations, by Chapter

Appendix 9—Statutory Provisions Related to Drop Boxes in Other States

Appendix 10—Number of Indefinitely Confined Individuals Who Voted Without Providing Photo Identification, by County

Appendix 11—Statutory Provisions Related to Permanent Absentee Voting for Individuals with Disabilities in Other States

Appendix 12—Clerks Who Indicated Receiving Written Complaints about the November 2020 General Election, By County

STATE OF WISCONSIN
Legislative Audit Bureau

Joe Chrisman
State Auditor

22 East Mifflin Street, Suite 500
Madison, Wisconsin 53703

Main: (608) 266-2818
Hotline: 1-877-FRAUD-17

www.legis.wisconsin.gov/lab
AskLAB@legis.wisconsin.gov

October 22, 2021

Senator Robert Cowles and
Representative Samantha Kerkman, Co-chairpersons
Joint Legislative Audit Committee
State Capitol
Madison, Wisconsin 53702

Dear Senator Cowles and Representative Kerkman:

As requested by the Joint Legislative Audit Committee, we have completed an evaluation of elections administration issues. The Wisconsin Elections Commission (WEC) is responsible for ensuring compliance with state and federal election laws. County and municipal clerks administer elections.

We reviewed the training that WEC is statutorily required to provide to municipal clerks, analyzed how WEC and clerks maintained the accuracy of voter registration records, reviewed guidance that WEC and its staff provided to clerks for handling absentee ballots and processing ballots, examined issues pertaining to electronic voting equipment and the statutorily required post-election audit that WEC conducted after the November 2020 General Election, assessed how WEC and its staff considered complaints, and examined the costs of the recount after the General Election.

To complete this audit, we contacted WEC's staff, surveyed all 1,835 municipal clerks and 72 county clerks in April 2021, contacted 179 clerks to obtain additional information about elections administration issues, analyzed voter registration data, physically reviewed 14,710 certificates that accompanied absentee ballots returned to clerks in 29 municipalities throughout the state, reviewed the results of 175 statutorily required tests of electronic voting equipment that clerks in 25 municipalities completed before the November 2020 General Election, and reviewed all 45 sworn, written complaints pertaining to the General Election that were filed with WEC as of late-May 2021.

We make 30 recommendations for improvements, which are located throughout the report and comprehensively listed in Appendix 7. We include 18 issues for legislative consideration, which are located throughout the report and comprehensively listed in Appendix 8.

We appreciate the courtesy and cooperation extended to us by WEC's staff, municipal clerks, and county clerks.

Respectfully submitted,

Joe Chrisman
State Auditor

JC/DS/ss

Introduction

WEC is responsible for ensuring compliance with state and federal election laws.

The Wisconsin Elections Commission (WEC) is responsible for ensuring compliance with state and federal election laws, and county and municipal clerks administer elections. Statutes require WEC to provide training and guidance to municipal clerks in the state's 1,849 municipalities. Statutes also require WEC to design and maintain the state's electronic voter registration system, which is known as WisVote; maintain the MyVote Wisconsin website, through which individuals may register to vote and obtain absentee ballots and other election-related information; and approve electronic voting equipment before it can be used in Wisconsin. Statutes specify how individuals can submit complaints pertaining to elections administration issues to WEC. WEC was created by 2015 Wisconsin Act 118, which was enacted in December 2015, and began operation on June 30, 2016. WEC replaced the Government Accountability Board (GAB), which was abolished by Act 118.

WEC includes six commissioners who serve for five-year terms, including:

- one commissioner appointed by the Senate Majority Leader;
- one commissioner appointed by the Senate Minority Leader;
- one commissioner appointed by the Assembly Speaker;
- one commissioner appointed by the Assembly Minority Leader; and

- two commissioners appointed by the Governor, with the advice and consent of the Senate. These two commissioners must have formerly served as county or municipal clerks. The Governor nominates one individual from each of the lists provided by the two political parties that received the most votes for President.

Appendix 1 lists the six WEC commissioners as of October 2021 and indicates how each commissioner was appointed.

WEC has delegated to the administrator limited authority to act without its involvement.

WEC is statutorily required to appoint an administrator with the advice and consent of the Senate. This administrator, who serves as the state's chief election officer, performs the duties assigned by WEC and appoints other staff as needed to help carry out these duties. Statutes require WEC's staff to be nonpartisan. WEC has delegated to the administrator limited authority to act without its involvement. In February 2020, WEC delegated the authority for the administrator to exempt municipalities from polling place accessibility requirements, exempt municipalities from using electronic voting equipment, and execute certain contracts up to $100,000. WEC also delegated the authority for the administrator to take specified actions in consultation with its chairperson, including when considering certain complaints.

Elections are administered by local election officials. Figure 1 shows the key statutory responsibilities of local election officials, including county clerks, municipal clerks, chief election inspectors, and election inspectors. The City of Milwaukee Election Commission, rather than the municipal clerk, administers elections in the City of Milwaukee.

Figure 1

Key Statutory Responsibilities of Local Election Officials

COUNTY CLERKS	MUNICIPAL CLERKS	CHIEF ELECTION INSPECTORS	ELECTION INSPECTORS
Prepare and provide ballots and election supplies	Register individuals to vote and administer elections	Direct the activities at polling places on Election Day	Serve at polling places to maintain order, ensure ballot boxes and poll lists are secure, and ensure that electronic voting equipment works properly; commonly known as "poll workers"
Section 7.10, Wis. Stats.	Section 7.15, Wis. Stats.	Section 7.36, Wis. Stats.	Section 7.37, Wis. Stats.

The Legislative Audit Bureau has previously completed audits of elections administration issues, including *Complaints Considered by the Government Accountability Board* (report 15-13), *Government Accountability Board* (report 14-14), *Compliance with Election Laws* (report 07-16), and *Voter Registration* (report 05-12).

After the General Election on November 3, 2020, questions were raised about elections administration issues, including compliance with election laws, the use of electronic voting equipment, and complaints filed with WEC and clerks. On February 11, 2021, the Joint Legislative Audit Committee directed us to evaluate elections administration issues, including:

- efforts by WEC to comply with election laws, including by working with clerks to ensure voter registration data include only eligible voters, and by providing training and guidance to clerks;

- efforts by clerks to comply with election laws, including by administering elections, processing absentee ballots, and performing recount responsibilities, as well as the observations and concerns of clerks regarding elections administration;

- the use of electronic voting equipment, including the methodology and results of WEC's most-recent statutorily required post-election audit and the actions taken as a result of this audit; and

- General Election–related complaints filed with WEC and clerks, as well as how those complaints were addressed.

To complete this evaluation of issues pertaining to the November 2020 General Election:

- We contacted eight groups that are involved with elections administration issues. These groups are listed in Appendix 2.

- We reviewed statutory provisions pertaining to elections administration and WEC's administrative rules. We contacted WEC's staff and reviewed their written policies and procedures, the minutes and materials associated with WEC's meetings, and the written guidance provided by WEC and its staff to municipal and county clerks.

- In April 2021, we invited all six WEC commissioners to discuss elections administration issues. Two commissioners spoke with us, and one other commissioner provided written information.

- In April 2021, we surveyed all 1,835 municipal clerks and all 72 county clerks to obtain their perspectives on various issues pertaining to the General Election. A total of 879 municipal clerks (47.9 percent) and 59 county clerks (81.9 percent) responded to our survey.

- We contacted a total of 179 clerks in 61 counties, including 157 municipal clerks and 22 county clerks, to obtain additional information about elections administration issues. The locations of these clerks are listed in Appendix 3.

- We analyzed WisVote data pertaining to voter registration records and absentee ballots cast in the General Election.

- We physically reviewed 14,710 absentee ballot certificates, which are typically the envelopes in which individuals return absentee ballots. We attempted to review certificates in 30 municipalities, including the 10 municipalities where the most absentee ballots were cast in the General Election, the 10 municipalities where the highest proportions of absentee ballots were cast in that election, and 10 municipalities we selected randomly from counties other than those in which the first 20 municipalities were located. However, the City of Madison clerk declined to allow us to physically handle the certificates. The clerk indicated that the clerk's office is responsible for maintaining the chain of custody of election records and ensuring these records are not inadvertently altered or damaged. As a result, we examined certificates in 29 municipalities. The results of our review are shown in Appendix 4.

- We reviewed a total of 1,233 Election Day forms completed by poll workers for the November 2020 General Election, including 571 forms completed by poll workers in 319 municipalities that we randomly selected and 662 forms completed by poll workers in 39 municipalities that had central count locations. On these forms, poll workers recorded information such as the numbers of absentee ballots that were remade and rejected. The results of our review are shown in Appendix 5.

- We reviewed a total of 175 statutorily required tests that municipal clerks had completed before the General Election for electronic voting equipment used in 25 municipalities. The results of our review are shown in Appendix 6.

- We reviewed all 45 sworn, written complaints pertaining to the General Election that were filed with WEC as of late-May 2021, and we reviewed 1,521 election-related concerns that individuals provided through forms on WEC's website from January 2020 through mid-April 2021.

- We assessed 26 reports that expressed general concerns about how the General Election was conducted and that were made to our office's Fraud, Waste, and Mismanagement Hotline. Few reports provided information pertaining to specific municipalities or issues. One report expressed concerns about a post-election investigation. We also assessed one complaint forwarded to us by a legislative office by speaking with two municipal clerks, but we did not find information to substantiate the issues in this complaint.

- We reviewed information about the recount costs that Dane and Milwaukee counties submitted to WEC after the General Election.

- We reviewed information from other states about various elections administration issues, including ballot drop boxes, signature verification on absentee ballot certificates, indefinitely confined individuals, post-election audits, and recount costs.

Based on our audit work, we make 30 recommendations for improvements and include 18 issues for legislative consideration.

Based on our audit work:

- we make 30 recommendations for improvements, which are located throughout the report and comprehensively listed in Appendix 7; and

- we include 18 issues for legislative consideration, which are located throughout the report and comprehensively listed in Appendix 8.

Because our audit was not approved until three months after the November 2020 General Election, we did not directly observe Election Day practices, including how poll workers processed ballots and how electronic voting equipment operated. The U.S. Department of Justice indicated that election officials are responsible for retaining and preserving election records, regardless of who physically possesses them. In part as a result of this guidance from the Department of Justice, the City of Madison clerk did not allow us to physically handle election records. In addition, county clerks indicated that we would not be able to handle ballots for Milwaukee County and the Town of Little Suamico. Combined, the City of Madison, Milwaukee County, and the Town of Little Suamico accounted for 623,700 of the 3.3 million ballots cast in the November 2020 General Election (18.9 percent). Therefore, to complete our audit we relied on available evidence we were able to

access, including WisVote data, absentee ballot certificates that we could physically handle, other election records, and information provided to us by municipal clerks, county clerks, WEC's staff, and other individuals.

Statutes require us at all times to observe the confidential nature of any audit being performed. As a result, we completed our audit independently from legislators, WEC, and all other individuals and organizations. Although we typically allow an audited entity the opportunity to review our draft audit report and respond in writing to it, we did not do so for this report. Because we contacted a total of 179 clerks, sharing the draft audit report with so many individuals would have compromised the report's confidentiality. In addition, because WEC's administrator has limited authority to act without WEC's involvement, we would have needed to provide our confidential draft audit report to WEC for its consideration. Statutes allow governmental bodies such as WEC to convene in closed session only for specified purposes, none of which pertains to reviewing draft audit reports. Thus, to preserve the statutorily required confidentiality of our audit until its completion, we did not provide WEC with an opportunity to review a confidential draft audit report and respond in writing to this report prior to its release.

■ ■ ■ ■

Training

Statutes require WEC to conduct regular training throughout the state for municipal clerks and other local election officials.

Statutes require WEC to conduct regular training throughout the state for municipal clerks and other local election officials. The training is intended to provide key information that clerks and other local election officials need to administer elections effectively, explain the state's election laws, and promote uniform procedures. WEC's staff train municipal clerks and the chief election inspectors who oversee individual polling places on Election Day, and they approve training provided by other entities. Municipal clerks are statutorily required to train other local election officials such as election inspectors, who are commonly known as poll workers. We reviewed training materials prepared by WEC's staff and contacted 20 clerks. We recommend WEC's staff work with WEC to promulgate and modify administrative rules and comply with the rules by notifying the governing bodies of municipalities when clerks have not reported that they completed the required training. We also include two issues for legislative consideration.

Municipal Clerks

Statutes require each municipal clerk to attend WEC-approved training at least once every two-year period that begins on January 1 of an even-numbered year and ends on December 31 of the following year. WEC's administrative rules require a clerk to attend three hours of training approved by WEC's staff in order to receive initial certification for the two-year period in which a clerk receives the training. A clerk must complete three additional hours of training, approved by WEC's administrator, in the same two-year period in order to maintain certification for the subsequent two-year period. Thereafter, a clerk

must attend six hours of approved training in a given two-year period in order to maintain certification for the subsequent two-year period. Statutes require WEC to promulgate administrative rules specifying the training contents. WEC's administrative rules require the training to address topics such as:

- completing election-related forms and notices;
- handling confidential voter information and proof of residence documents;
- acquiring, testing, and auditing voting equipment;
- ensuring the security of ballots and voting equipment; and
- preparing and supplying polling places.

We reviewed WEC's election administration manual and materials for the three-hour training that municipal clerks must complete in order to obtain initial certification. We found that the training and the manual, which is referenced in the training, addressed all of the training provisions specified by WEC's administrative rules.

WEC's administrative rules for training municipal clerks have not been updated since June 2016 and contain outdated provisions.

We found that WEC's administrative rules for training municipal clerks have not been updated since June 2016 and contain outdated provisions. The administrative rules specify that training may include how municipal clerks are to use the former Statewide Voter Registration System (SVRS), which was replaced by WisVote in January 2016. The administrative rules also require clerks to complete training during two-year periods that begin on January 1 of odd-numbered years, rather than the even-numbered years required by statutes. WEC's staff should work with WEC to modify administrative rules to reflect current statutory requirements for elections, such as training clerks on how to use WisVote.

☑ Recommendation

We recommend staff of the Wisconsin Elections Commission:

- *work with the Wisconsin Elections Commission to modify ch. EL 12, Wis. Adm. Code, to reflect current statutory requirements for elections; and*
- *report to the Joint Legislative Audit Committee by March 31, 2022, on their efforts to implement this recommendation.*

WEC's staff provided municipal clerks with training in coordination with organizations such as the Wisconsin Towns Association and the Wisconsin Municipal Clerks Association. WEC's staff provided us with information indicating that training occurred at locations throughout the state in the months before mid-March 2020, when they ceased to provide in-person training as a result of the public health emergency and instead provided training online. WEC's staff conducted:

- 20 sessions on electronic poll books in December 2019 and January 2020;
- 12 sessions on election security from January 2020 through mid-March 2020; and
- 5 tabletop exercises on election security in December 2019 and January 2020.

To increase training opportunities for municipal clerks, WEC's staff trained and certified county and municipal clerks to be clerk-trainers. For the current two-year training period that began in January 2020, WEC's staff certified nine individuals, including seven county clerks and two municipal clerks, to provide the training that municipal clerks need to obtain initial certification.

Compliance with Training Requirements

As of June 2021, 82.5 percent of municipal clerks who served in those positions before January 2020 reported having completed all required training.

WEC's staff relied on municipal clerks to self-report the number of training hours that the clerks completed. WEC's staff provided us with information for the two-year period from January 2018 through December 2019, which was the most recently completed training period at the time of our audit. Clerks who completed all required training during this period were certified for the two-year period that began in January 2020. As of June 2021, the information indicated that 175 clerks had started in their positions in January 2020 or later and, therefore, were not required to complete any training in the previous period, and 1 clerk position was vacant. Of the remaining 1,636 clerks who had served in those positions before January 2020:

- 1,349 municipal clerks (82.5 percent) reported having completed all required training; and
- 287 municipal clerks (17.5 percent) did not report having completed all required training.

We reviewed information on the training that municipal clerks reported having completed from January 1, 2020, through November 3, 2020. This information reflected training reported to WEC's staff as of June 2021. We found that 874 clerks reported having completed some training. These clerks reported having each completed an average of 6.7 hours of training.

We attempted to determine the extent to which individuals who began working as municipal clerks in 2020 had completed the initial training before the November 2020 General Election. However, statutes do not require individuals to inform WEC of the dates they began working as clerks, and WEC's staff indicated that they are not consistently informed of these dates.

WEC's staff provided us with training information reported by 120 municipal clerks who, to the knowledge of WEC's staff, began working in those positions in 2020. This information reflected training reported as of June 2021. We found that:

- 76 clerks (63.3 percent) reported having each completed, on average, 6.0 hours of training from January 1, 2020, through November 3, 2020, including 71 clerks who reported having completed the initial training; and

- 44 clerks (36.7 percent) did not report having completed any training from January 1, 2020, through November 3, 2020. Some of these clerks may have completed training but did not report it, and some may have begun working as clerks after November 3, 2020.

WEC's staff did not comply with administrative rules because they did not contact governing bodies if clerks did not report having completed the required training for the two-year period that ended in December 2019.

Statutes require WEC to promulgate administrative rules that include a method for notifying the governing body of a given municipality if a municipal clerk does not complete the required training. WEC's administrative rules state only that WEC will notify a governing body if a clerk does not complete the training. WEC's staff indicated that they did not contact any governing bodies if clerks did not report having completed the required training for the two-year period that ended in December 2019. Instead, WEC's staff indicated that they contacted clerks and attempted to elicit their cooperation in completing and reporting the training. In addition, WEC's staff posted information on WEC's website about the amount of training that clerks reported having completed in the two-year period that ended in December 2019. This information could be misleading because it included clerks who began in their positions after that two-year period had ended and, therefore, were not expected to have completed any training during that two-year period.

WEC's staff should work with WEC to modify administrative rules to specify how they will notify the governing bodies of municipalities when clerks do not report having completed training required by administrative rules. WEC's staff should then consistently comply with administrative rules. Doing so may provide greater assurance that the training is completed and reported.

☑ Recommendation

We recommend staff of the Wisconsin Elections Commission:

- *work with the Wisconsin Elections Commission to modify ch. EL 12.02 (7), Wis. Adm. Code, to specify how the governing bodies of municipalities will be notified when municipal clerks do not report having completed training required by administrative rules;*
- *consistently comply with administrative rules; and*
- *report to the Joint Legislative Audit Committee by March 31, 2022, on their efforts to implement these recommendations.*

Issues for Legislative Consideration

The Legislature could consider modifying statutes to require clerks to complete the initial training before administering an election.

Currently, statutes require municipal clerks to attend training at least once every two years, and WEC's administrative rules require clerks to complete three hours of training in order to receive initial certification for the two-year period in which the training is received. However, statutes and administrative rules do not specify when a new clerk must complete the training for initial certification, and they do not require clerks to be certified before administering an election for the first time. As a result, a clerk could administer an election before having completed the initial training. The Legislature could consider modifying statutes to require clerks to complete the initial training before administering an election. Statutes could exempt from this training requirement those individuals who became clerks only shortly before an election.

The Legislature could consider modifying statutes to require a municipal governing body to notify WEC within 30 days when there is turnover in the clerk position.

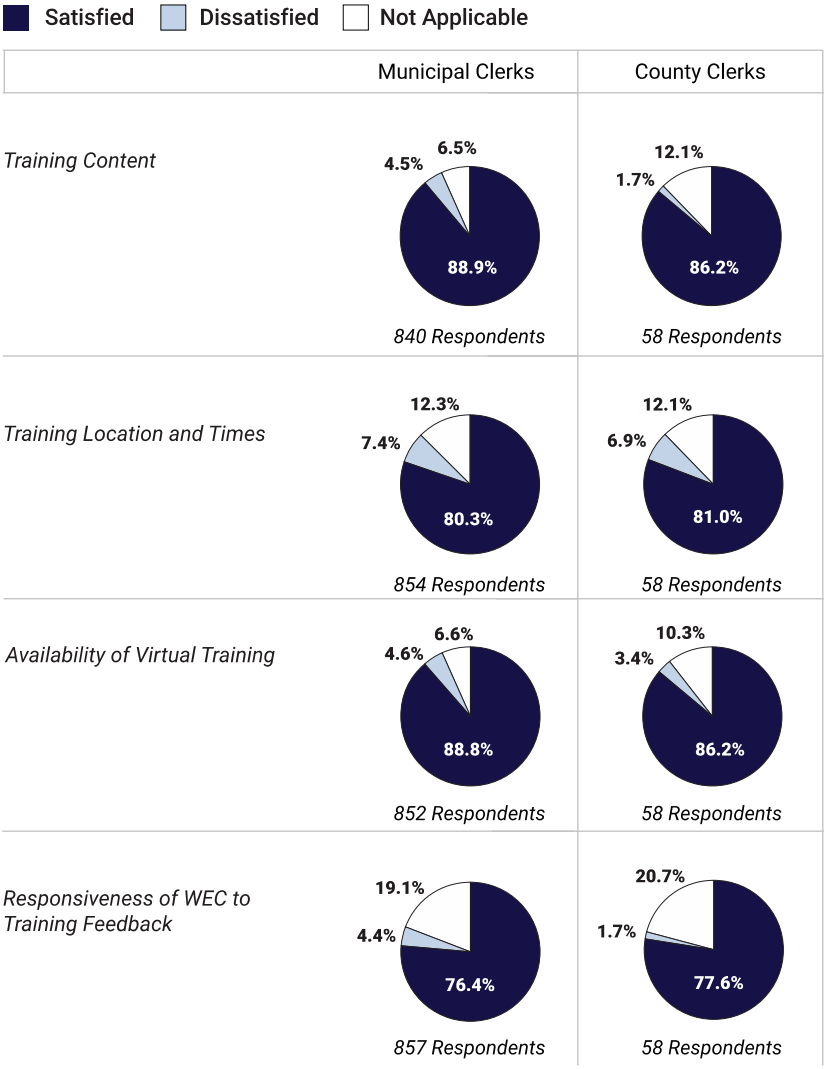
Currently, statutes do not require individuals to inform WEC of the dates they began working as municipal clerks, and WEC's staff indicated that they are not consistently informed of these dates. The Legislature could consider modifying statutes to require a municipal governing body to notify WEC within 30 days when there is turnover in the clerk position. If WEC were better informed, it could more accurately track whether clerks completed all required training.

Satisfaction Levels of Clerks

Our April 2021 survey asked municipal and county clerks about the training provided by WEC's staff. As shown in Figure 2, most clerks who responded to our survey indicated that they were satisfied with the training content, training location and times, availability of virtual training, and the responsiveness of WEC to feedback on the training.

Figure 2

Satisfaction of Clerks with Training Provided by WEC's Staff[1]

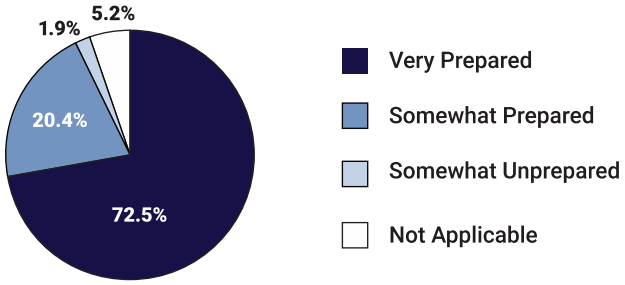


[1] As indicated by municipal and county clerks who responded to our April 2021 survey.

As shown in Figure 3, 72.5 percent of the municipal clerks who responded to our survey indicated they were very prepared to fulfill their duties in the November 2020 General Election as a result of training provided by WEC, and 20.4 percent indicated that they were somewhat prepared.

Figure 3

Clerk Preparedness for the November 2020 General Election, as a Result of WEC's Training[1]



[1] As indicated by 858 municipal clerks who responded to our April 2021 survey.

We contacted 16 municipal clerks and 4 county clerks to obtain their perspectives on WEC's training. Similar to our survey, these clerks indicated that they were generally satisfied with the training. For example:

- one clerk indicated that there were adequate training opportunities and that WEC's staff did a good job using technology to deliver training virtually;
- a second clerk indicated that the training covered all necessary topics; and
- a third clerk indicated that WEC's staff did a good job providing training and other resources for clerks to obtain needed information.

We also contacted clerks who had indicated in their survey responses that they were dissatisfied with the training. For example:

- one clerk indicated that the training and guidance were contradictory at times;
- a second clerk indicated that the training was more useful for clerks in larger municipalities; and
- a third clerk indicated that the training should cover more topics and that WEC should improve WEC's election administration manual.

Other Local Election Officials

Other local election officials help municipal clerks to administer elections. Chief election inspectors serve as the lead election official at polling places, election inspectors perform various duties at polling places, and special voting deputies visit residential care facilities and qualified retirement homes in order to conduct absentee voting in person.

Chief Election Inspectors

Statutes require municipal clerks to appoint an individual to serve as the chief election inspector at a given polling place. Statutes require WEC to establish requirements for certifying individuals to serve as chief election inspectors, including the requirement to attend at least one training session before serving as a chief election inspector. Individuals may not serve as chief election inspectors unless WEC certifies them. To maintain certification, chief election inspectors must attend at least one training session during every two-year period that begins on January 1 of each even-numbered year and ends on December 31 of the following year.

WEC's staff indicated that municipal clerks are responsible for ensuring that individuals who serve as chief election inspectors meet the training requirements and are certified. In the current two-year training period that began in January 2020, WEC's staff certified 47 individuals, including county clerks, municipal clerks, deputy clerks, and others, to provide baseline training to chief election inspectors. In response to the public health emergency, WEC's staff made this training publicly available on WEC's website.

We reviewed the chief election inspector training and found that it included a variety of topics related to administering an election, including conducting pre-election tests of electronic voting equipment, opening and closing polls, registering voters, processing absentee ballots, and completing election forms.

Chief election inspectors sign Election Day forms certifying that they had previously completed the required training and are certified. After Election Day, county clerks maintain these forms. We selected a random sample of 319 municipalities throughout the state and requested that the clerks of the 69 counties where these municipalities are located provide us with the forms completed for the November 2020 General Election. We reviewed all 571 forms provided to us and found that 567 forms (99.3 percent) contained signatures of chief election inspectors.

Other Election Officials

Statutes require WEC to promulgate administrative rules prescribing the contents of training that municipal clerks provide to other local

election officials, including election inspectors and special voting deputies. In report 14-14, we found that GAB had approved draft administrative rules regarding the contents of training for election inspectors and special voting deputies and in August 2009 had directed its staff to complete the promulgation process. We also found that GAB's staff had not done so through September 2014 but had instead relied on election manuals to indicate the training contents. We recommended that GAB promulgate the statutorily required administrative rules.

WEC did not comply with statutes by promulgating administrative rules prescribing the contents of training for special voting deputies or election inspectors.

In our current audit, we found that WEC did not promulgate statutorily required administrative rules prescribing the contents of training for special voting deputies or election inspectors. WEC's staff indicated that they were unaware of any discussions WEC had regarding promulgating the statutorily required administrative rules. Instead, WEC's staff provided municipal clerks with written guidance on training special voting deputies and election inspectors.

WEC's staff should work with WEC to promulgate the statutorily required administrative rules regarding the contents of training that municipal clerks provide to special voting deputies and election inspectors. Although the written guidance that WEC's staff provided municipal clerks contained relevant information, provisions in administrative rules carry the force of law.

☑ Recommendation

We recommend staff of the Wisconsin Elections Commission:

- *work with the Wisconsin Elections Commission to promulgate statutorily required administrative rules prescribing the contents of training that municipal clerks provide to special voting deputies and election inspectors; and*

- *report to the Joint Legislative Audit Committee by March 31, 2022, on their efforts to implement this recommendation.*

■ ■ ■ ■

Maintenance of Voter Registration Records

WEC and clerks share responsibility for maintaining the accuracy of voter registration records.

WEC and clerks share responsibility for maintaining the accuracy of voter registration records. Statutes require WEC to maintain WisVote and municipal clerks to use WisVote to verify the accuracy of information provided by registrants, who are individuals registering to vote. Information provided by registrants is matched with personally identifiable information from the Department of Transportation (DOT). WEC obtains personally identifiable information from the departments of Health Services (DHS) and Corrections (DOC) and provides it to clerks. Clerks use this information to inactivate the voter registration records of individuals ineligible to vote because they are deceased or have ongoing felony sentences. We recommend WEC's staff work with WEC to execute written data-sharing agreements with these three state agencies, improve how they identify potentially duplicate voter registration records in WisVote, and establish a schedule for regularly obtaining data from the Electronic Registration Information Center (ERIC), which is a nonprofit organization that helps member states to improve the accuracy of their voter registration systems by providing personally identifiable information on certain types of individuals. We also include two issues for legislative consideration.

Voter Registration

Any U.S. citizen age 18 or older is eligible to vote in a Wisconsin election district where he or she has resided for 28 consecutive days before an election, if he or she has not been determined by a judge to be incompetent to vote, has not bet on the election, and is not serving a sentence for a felony, treason, or bribery.

Almost one-half of the 957,977 individuals who registered to vote in Wisconsin from January 1, 2020, through November 3, 2020, did so online.

Statutes allow individuals to register to vote at any time except for the three days before Election Day. Individuals who register 20 days or more before Election Day may typically do so online through the MyVote Wisconsin website, at a clerk's office, or by mail. Individuals who register within 20 days before Election Day may typically do so only at a municipal clerk's office or on Election Day at the polls. As shown in Table 1, almost one-half of the 957,977 individuals who registered to vote in Wisconsin from January 1, 2020, through November 3, 2020, did so online.

Table 1

Individuals Who Registered to Vote, by Method[1]
January 1, 2020, through November 3, 2020

Method	Number of Individuals	Percentage of Total
Online	476,605	49.8%
In Person	423,282	44.2
Mail[2]	58,090	6.1
Total	**957,977**	**100.0%**

[1] According to information that clerks entered into WisVote.

[2] Includes individuals who registered by email or fax.

Statutes require municipal clerks to enter information provided by individuals registering to vote by mail or in person into WisVote. Statutes allow any municipal clerk to designate another municipal clerk or a county clerk to enter such information into WisVote on the clerk's behalf. As of March 2021, 1,155 municipalities (62.5 percent) had arrangements with their counties or other municipalities for assistance in entering information into WisVote, including voter registration–related information.

Personally Identifiable Information

Registrants must provide their valid driver's license numbers or state identification card numbers, but they may provide the last four digits of their Social Security numbers if they do not have valid driver's licenses or state identification cards. Registrants must also provide their dates of birth and current addresses.

Statutes require WEC's administrator and DOT's secretary to enter into an agreement to attempt to verify the personally identifiable information provided by registrants with DOT's information.

Statutes require WEC's administrator and DOT's secretary to enter into an agreement to attempt to verify the personally identifiable information provided by registrants with DOT's information on vehicle registrations, driver's licenses, and state identification cards. Each night, the personally identifiable information of individuals who registered to vote is electronically compared with DOT's information, including names, dates of birth, and driver's license or state identification card numbers. If registrants do not provide driver's license or state identification card numbers, DOT forwards the last four digits of their Social Security numbers to the federal Social Security Administration, which compares this information with its records. DOT electronically informs WEC whether it confirmed the information provided by registrants. If DOT did not confirm this information, it electronically informs WEC about the particular piece of information it could not confirm. However, DOT does not provide WEC with any personally identifiable information, such as names or dates of birth.

If an individual registers to vote online, statutes require the personally identifiable information provided by individuals to be instantly verified with DOT's information. If the information cannot be verified, statutes require individuals to be redirected to DOT's website in order to update their information. Individuals cannot complete their online registrations until the information they provide matches DOT's information.

The personally identifiable information provided by 93.8 percent of individuals who registered to vote matched DOT's information.

We used data provided by WEC's staff to determine the extent to which the personally identifiable information provided by individuals who registered to vote from January 1, 2020, through November 3, 2020, matched DOT's information. As shown in Table 2, the information provided by 93.8 percent of these 957,977 individuals matched DOT's information, but the information provided by 4.8 percent of these individuals did not. In report 14-14, we found that information provided by 92.4 percent of individuals who registered to vote in fiscal year (FY) 2012-13 matched DOT's information, but that 7.4 percent did not.

Table 2

Comparison of Personally Identifiable Information Provided by Individuals Registering to Vote with DOT's Information[1]
January 1, 2020, through November 3, 2020

	Number of Individuals	Percentage of Total
The Information:		
Matched DOT's Information	898,421	93.8%
Did Not Match DOT's Information	45,665	4.8
No Attempt Was Made to Match the Information	13,800	1.4
The Match Was Ongoing	91	<0.1
Total	**957,977**	**100.0%**

[1] As indicated by data provided by WEC's staff.

Non-matches occurred for 63.1 percent of the 45,665 individuals because the names the individuals provided when registering to vote did not match DOT's information. WEC's staff indicated that a non-match could have occurred if, for example, an individual registered to vote as "Robert" but was known as "Bob" on a driver's license. However, the data do not indicate precisely why the non-match occurred because DOT does not provide WEC with any personally identifiable information. As a result, clerks are uncertain whether a non-match occurred because of only a slight difference in a given individual's name, which may indicate little cause for concern, or a significant difference, which may indicate that an individual is attempting to register to vote by using another individual's information.

WEC's staff indicated that no attempts were made to match the personally identifiable information provided by 13,800 individuals for several reasons. Individuals serving in the military are not statutorily required to register to vote and, thus, do not provide driver's license, state identification card, or Social Security numbers, although WisVote contains voter records for these individuals. Similarly, no matching attempts were made if individuals updated registrations that had previously been made before WisVote's implementation and the individuals were not changing their names, driver's license or Social Security numbers, or dates of birth.

If the personally identifiable information provided by registrants does not match DOT's information, the relevant clerks receive automatic notifications in WisVote. WEC's staff instruct clerks to correct the voter registration if they can determine that the non-match was the result of a data entry error. Otherwise, clerks are instructed to inform the individuals that they should resolve the mismatched information.

Statutes do not require clerks to inactivate the voter registration records of these individuals, who remain eligible to vote.

We contacted a total of 12 municipal and county clerks in order to learn how they reviewed instances when information provided by registrants did not match DOT's information. The clerks indicated that they typically reviewed the available information in order to determine why a non-match may have occurred. For example, they may discover a typo in the registration information that could have caused a non-match. However, one county clerk was unaware of the need to review non-matches, and one municipal clerk indicated not having time to review non-matches.

Data Agreement

WEC did not have a written data-sharing agreement with DOT at the time of our audit.

We found that WEC did not have a written data-sharing agreement with DOT at the time of our audit. The most-recent agreement was effective from January 5, 2017, until January 5, 2021. This agreement pertained only to verifying information provided by individuals who registered online to vote, and not to verifying information provided by individuals who registered to vote by other methods. WEC's staff indicated that they planned to update the agreement later in 2021.

We found that WEC's data-sharing agreement, which expired on January 5, 2021, did not specify any procedures that DOT should use to verify information provided by individuals who registered to vote by methods other than online. Instead, WEC's staff indicated that verification occurs based on procedures formally agreed upon with DOT in 2005.

WEC did not comply with statutes by obtaining from DOT the signatures of individuals who register online to vote.

Statutes require individuals who register online to vote to authorize WEC to obtain from DOT electronic copies of the signatures they provided when they obtained driver's licenses or state identification cards. Statutes require WEC to obtain these signatures. However, we found that WEC's most-recent agreement with DOT explicitly did not include the provision of these signatures. WEC's staff indicated that no signatures were obtained from DOT, in part, because a significant amount of electronic space would be needed to store them. DOT indicated that an individual's signature and photo are stored in one file, which could make it challenging to provide WEC with only the signatures.

Before January 1, 2022, WEC's staff should work with WEC to execute a new written data-sharing agreement with DOT. This agreement should include provisions for verifying the information provided by individuals who register to vote by all methods, and it should specify the procedures for verifying this information. WEC's staff should also establish a system to regularly review and update the agreement with DOT. Doing so will ensure that the data-sharing process reflects current technological processes and available data, and that the agreement does not expire in the future without a replacement agreement. In addition, WEC's staff should comply with statutes by working with DOT to obtain the electronic signatures of individuals who register online to vote. If WEC believes that such signatures cannot help it to ensure the

accuracy of voter registration records, it should request that the Legislature modify the statutory requirement that it obtain the signatures.

☑ Recommendation

We recommend staff of the Wisconsin Elections Commission:

- *before January 1, 2022, work with the Wisconsin Elections Commission to execute with the Department of Transportation a new written data-sharing agreement that includes provisions for verifying the information provided by individuals who register to vote by all methods and that specifies the procedures for verifying this information;*

- *establish a system to regularly review and update the data-sharing agreement;*

- *comply with statutes by working with the Department of Transportation to obtain the electronic signatures of individuals who register online to vote, or request that the Legislature modify the statutory requirement that the Wisconsin Elections Commission obtain them; and*

- *report to the Joint Legislative Audit Committee by March 31, 2022, on their efforts to implement these recommendations.*

Issue for Legislative Consideration

The Legislature could consider modifying statutes to require that DOT provide additional information to WEC when DOT attempts to verify certain information provided by registrants.

As noted, DOT currently provides information that does not indicate precisely why a given non-match occurred because DOT does not provide WEC with any personally identifiable information. The Legislature could consider modifying statutes to require that DOT provide additional information to WEC when DOT attempts to verify the personally identifiable information provided by registrants. For example, statutes could be modified to require DOT to provide WEC with the names, dates of birth, and driver's license or state identification card numbers for individuals whose information did not match. WEC's staff and clerks we contacted indicated that this additional information would help them to identify and correct errors in voter registration records, such as misspelled names and typos.

Duplicate Voter Registration Records

Each night, WisVote automatically compares personally identifiable information in voter registration records in order to identify potentially duplicate records.

Each night, WisVote automatically compares certain personally identifiable information in voter registration records in order to identify potentially duplicate records. The relevant clerks receive automatic notifications in WisVote whenever the information in one record matches the information in another record. When this occurs, WEC's staff instruct clerks to consider the available information and either merge the two records or determine a potential match was erroneous and allow the two records to remain separate. WisVote uses four sets of criteria to identify potentially duplicate records.

Duplicate voter registration records can be identified with additional sets of criteria not currently used by WisVote. We used only the driver's license and state identification card numbers to identify potentially duplicate records for all individuals who voted absentee in the November 2020 General Election. We identified 70 records in which either driver's license or state identification card numbers matched the numbers in 70 separate records. We provided WEC's staff with a list of these 140 total records for their review because the criteria WEC's staff use to identify potentially duplicate records would not have discovered these records.

We provided WEC's staff with the names of four individuals who may have voted twice by absentee ballot during the November 2020 General Election.

We found that the names and dates of birth of the individuals associated with 24 of the 70 voter registration records that we identified by using our criteria matched similar information in 24 other records. This suggests that the 24 individuals associated with these records had two active voter registration records. We analyzed absentee ballot data provided by WEC's staff and found that these data indicated 4 of the 24 individuals may have voted twice by absentee ballot during the November 2020 General Election. We provided WEC's staff with the names of these 24 individuals, including the 4 individuals who may have voted twice.

WEC's staff should improve how they identify potentially duplicate voter registration records in WisVote by comparing driver's license and state identification card numbers of all registered voters each night. Because driver's license and state identification card numbers should be unique, clerks should merge duplicate records or correct any information that resulted in the matches. For example, a mistyped driver's license number may have resulted in an erroneous match. Taking these actions will improve the accuracy of voter registration records.

☑ Recommendation

We recommend staff of the Wisconsin Elections Commission:

- *improve how they identify potential duplicate voter registration records in WisVote by comparing driver's license and state identification card numbers of all registered voters each night; and*

- *report to the Joint Legislative Audit Committee by March 31, 2022, on their efforts to implement this recommendation.*

Deceased Individuals

Each month, DHS electronically provides WEC with personally identifiable information for all Wisconsin residents who died in the state.

Statutes require municipal clerks to use vital statistics reports to inactivate the voter registration records of deceased individuals. On an ongoing basis, DHS receives information about deceased individuals, primarily from funeral homes. Each month, DHS electronically provides WEC with personally identifiable information for all Wisconsin residents who died in the state, including names, last four digits of Social Security numbers, dates of birth and death, and the cities and counties where these individuals last lived. By the time that WEC obtains this information, varying amounts of time have elapsed.

WisVote automatically compares the information provided by DHS with the personally identifiable information in voter registration records, as well as with the personally identifiable information provided by registrants. The relevant clerks receive automatic notifications in WisVote whenever the information provided by DHS potentially matches the personally identifiable information in voter registration records. WEC's staff instruct clerks to consider the available information and either inactivate a given record or determine the potential match was erroneous and allow a given record to remain active. WisVote indicates whether clerks used the potential matches to make such determinations. In report 14-14, we found that clerks had acted on 93.6 percent of potential matches provided by DHS in FY 2012-13, but that clerks had not acted on 6.4 percent of potential matches.

We obtained data from WEC's staff on all 33,473 potential matches between the information provided by DHS and the personally identifiable information in voter registration records from January 1, 2020, through November 3, 2020. These data indicated whether clerks had acted on the potential matches as of mid-April 2021. If a clerk does not act on a potential match for a given individual, WEC's staff are uncertain if a clerk determined whether an individual is still alive and, therefore, whether the voter registration record is accurate.

Clerks did not consistently act on potential matches provided by DHS to inactivate the voter registration records of individuals who may have died.

As shown in Table 3, the data indicated that clerks had acted on the potential matches for 20,908 individuals (62.5 percent), but that clerks in 1,199 municipalities had made no determinations on the potential matches for 12,565 individuals (37.5 percent). Although the data indicated that clerks had not acted on the potential matches, other data provided by WEC's staff indicated that, in fact, clerks had inactivated the records of 12,406 of the 12,565 individuals (98.7 percent) as of the November 2020 General Election and had inactivated the records of all but 8 of the 12,565 individuals as of June 2021. To inactive these records, clerks used information sources other than the potential matches. In response to our April 2021 survey, 188 municipal clerks indicated that they had inactivated records before the General Election, including 144 clerks who relied on obituaries, 72 clerks who relied on personal knowledge about individuals, and 49 clerks who inactivated

records after individuals did not respond to mailed notices about their potential ineligibility to vote.

Table 3

Resolution of Information Indicating That Registered Voters Were Deceased[1]
January 1, 2020, through November 3, 2020

	Number of Individuals	Percentage of Total
Clerks Determined Individuals Were:		
Deceased	20,614	61.6%
Alive	294	0.9
Subtotal	20,908	62.5
Clerks Made No Determinations[2]	12,565	37.5
Total	**33,473**	**100.0%**

[1] As indicated by data that were provided by WEC's staff and that indicated the determinations clerks had made as of mid-April 2021.

[2] As of June 2021, clerks had inactivated the voter registration records of all but 8 of the 12,565 individuals.

If an individual submits an absentee ballot but dies before Election Day, statutes require that the absentee ballot not be counted if local election officials are aware of the death. Identifying deceased individuals in time to ensure that their absentee ballots are not counted is sometimes challenging because of the amount of time required for DHS to be notified of the deaths, for DHS to prepare the applicable data, and for the monthly data exchange with WisVote to occur. We found that it took clerks a median time of:

- 7 days from when they were informed about a potential match to when they determined that an individual was deceased or alive; and
- 56 days from when individuals died to when they determined that an individual was deceased or alive.

Eleven individuals who died before November 3, 2020, likely voted in the General Election.

We reviewed the voting records of the 20,614 individuals who clerks determined were deceased and the 12,565 individuals for whom clerks made no determinations. The available information indicates that 11 individuals who died before November 3, 2020, likely voted in the General Election. Clerks received potential data matches for all 11 individuals 10 days before the General Election. By that point in time, clerks had mailed absentee ballots to all 11 individuals. We notified WEC's staff about these 11 individuals.

Data Agreement

WEC did not have a written data-sharing agreement with DHS at the time of our audit.

We found that WEC did not have a written data-sharing agreement with DHS at the time of our audit. The most-recent agreement was effective from January 1, 2016, through December 31, 2016.

Before January 1, 2022, WEC's staff should work with WEC to execute a new written data-sharing agreement with DHS, and they should establish a system to regularly review and update the agreement. Doing so will ensure that the data-sharing process reflects current technological processes and available data, and that the agreement does not expire in the future without a replacement agreement.

☑ Recommendation

We recommend staff of the Wisconsin Elections Commission:

- *before January 1, 2022, work with the Wisconsin Elections Commission to execute a new written data-sharing agreement with the Department of Health Services;*
- *establish a system to regularly review and update the data-sharing agreement; and*
- *report to the Joint Legislative Audit Committee by March 31, 2022, on their efforts to implement these recommendations.*

Individuals Serving Felony Sentences

DOC is statutorily required on a continuous basis to provide WEC with information on individuals who have been convicted of felonies.

Statutes prohibit individuals convicted of felonies from voting until they have completed their sentences, including parole and extended supervision, or completed probation. DOC is statutorily required on a continuous basis to provide WEC with the names and addresses of individuals who have been convicted of felonies and whose civil rights have not been restored, as well as the dates DOC expects these civil rights to be restored.

Each day, WisVote automatically compares the information provided by DOC with the personally identifiable information in voter registration records. The relevant clerks receive automatic notifications in WisVote whenever the information provided by DOC potentially matches information in voter registration records. WEC's staff instruct clerks to consider the available information and either inactivate a given record or determine the potential match was erroneous and allow a given record to remain active. WEC's staff indicated that clerks need to carefully consider potential matches because DOC's information changes frequently and can contain duplicate records. In report 14-14, we found that clerks had acted on 91.8 percent of potential matches

provided by DOC in FY 2012-13, but that clerks had not acted on 8.2 percent of potential matches.

We obtained data on all potential matches between DOC's information and the personally identifiable information in voter registration records from January 1, 2020, through November 3, 2020. We determined the extent to which clerks had acted on these potential matches as of mid-April 2021. If a clerk does not act on a potential match for a given individual, WEC's staff are uncertain whether a clerk determined whether an individual has an ongoing felony sentence and, therefore, whether the voter registration record is accurate.

Clerks did not consistently act on the potential match information provided by DOC to inactivate the voter registration records of individuals who may have been serving felony sentences.

As shown in Table 4, the data indicated that clerks had acted on the potential matches for 1,435 individuals (63.6 percent), and it took a median time of five days to act on these matches. Clerks in 296 municipalities had made no determinations on the potential matches for 821 individuals (36.4 percent). Although the data indicated that clerks had not acted on the potential matches, other data provided by WEC's staff indicated that, in fact, clerks had inactivated the records of 748 of the 821 individuals (91.1 percent) as of the November 2020 General Election and had inactivated the records of all but 1 of the 821 individuals as of September 2021.

Table 4

Resolution of Information Indicating That Registered Voters Had Ongoing Felony Sentences[1]
January 1, 2020, through November 3, 2020

	Number of Individuals	Percentage of Total
Clerks Determined Individuals:		
Had Ongoing Felony Sentences	1,115	49.4%
Did Not Have Ongoing Felony Sentences	320	14.2
Subtotal	1,435	63.6
Clerks Made No Determinations[2]	821	36.4
Total	**2,256**	**100.0%**

[1] As indicated by data that were provided by WEC's staff and that indicated the determinations clerks had made as of mid-April 2021.

[2] As of September 2021, clerks had inactivated the voter registration records of all but 1 of the 821 individuals.

Eight individuals with ongoing felony sentences may have voted in the General Election.

We reviewed the voting records of the 1,115 individuals whom clerks determined had ongoing felony sentences and the 821 individuals for whom clerks made no determinations. We found that the available data indicate that eight individuals with ongoing felony sentences may have voted in the November 2020 General Election. Clerks had

received information about the potential matches for four of these eight individuals within 30 days before the General Election. WEC's staff were aware of all eight individuals based on their own post-election review conducted independently from our audit.

We selected a random sample of 75 of the 1,115 individuals whose voter registration records clerks inactivated. We reviewed the Wisconsin Court System's Consolidated Court Automation Programs (CCAP) and found that the available information indicated the felony sentences of 3 of the 75 individuals had ended before the November 2020 General Election. We provided WEC's staff with the names of these individuals.

Data Agreement

To obtain information on individuals with ongoing felony sentences, GAB executed a data-sharing agreement of indefinite duration with DOC in October 2015. Although GAB executed this agreement, 2015 Wisconsin Act 118 stipulated that all ongoing contracts remained in effect after GAB was abolished.

WEC's data-sharing agreement with DOC contained outdated information.

We found that WEC's data-sharing agreement with DOC contained outdated information. The agreement referenced SVRS, which has been replaced by WisVote. In addition, WEC's staff indicated that the technology for transferring data between the two agencies was updated in recent years and that additional updates are anticipated. Although the agreement specified it was to be reviewed at least annually, WEC's staff indicated that such reviews did not occur.

Before January 1, 2022, WEC's staff should work with WEC to update the almost six-year-old data-sharing agreement with DOC, and they should establish a system to regularly review and update the agreement. Doing so will ensure that the data-sharing process reflects current technological processes and available data.

☑ Recommendation

We recommend staff of the Wisconsin Elections Commission:

- *before January 1, 2022, work with the Wisconsin Elections Commission to execute a new data-sharing agreement with the Department of Corrections;*
- *establish a system to regularly review and update the data-sharing agreement; and*
- *report to the Joint Legislative Audit Committee by March 31, 2022, on their efforts to implement these recommendations.*

Post-Election Review

After every election, statutes require WEC to compare the list of individuals provided by DOC with the list of individuals who registered to vote on Election Day or within 20 days before an election. If WEC determines that an individual with an ongoing felony sentence may have voted, statutes require it to notify the district attorney in the county where the vote occurred. Statutes require WEC to complete these reviews as soon as possible.

WEC's staff completed statutorily required post-election reviews for every election from June 2016 through November 2020.

In report 14-14, we found that GAB's staff had not completed these statutorily required reviews for several years, and we recommended that they be completed. In our current audit, we found that WEC's staff had completed these reviews for every election from WEC's inception in June 2016 through the November 2020 General Election, although some cases pertaining to the General Election were in the process of being reviewed by clerks at the time of our audit.

Electronic Registration Information Center (ERIC)

2015 Wisconsin Act 261, which was enacted in March 2016, requires WEC to belong to ERIC. As of March 2020, 30 states and the District of Columbia were members of ERIC. Member states such as Wisconsin provide ERIC with personally identifiable information from their voter registration and driver's license systems. ERIC also collects personally identifiable information from the Social Security Administration and the U.S. Postal Service. Each member state decides how often to request data from ERIC, but ERIC requires each state to request some data at least annually.

WEC can request that ERIC provide it with five types of data.

Under the terms of its agreement with ERIC, WEC can request that ERIC provide it with data containing personally identifiable information on:

- eligible Wisconsin residents who are not registered to vote;
- registered Wisconsin voters who may have moved within Wisconsin, who may have moved to and registered to vote in other states, or who submitted new address information to the U.S. Postal Service's National Change of Address program;
- registered Wisconsin voters who may have voted multiple times in the same election;
- registered Wisconsin voters who may have died in other states; and

- registered Wisconsin voters who may have multiple voter registration records in Wisconsin.

Some types of ERIC data are available to WEC through other sources, such as data on voters who may have moved within Wisconsin. Nevertheless, WEC's staff indicated that ERIC's data-matching software is better than WEC's software at identifying individuals whose voter registration records may need to be inactivated or who may have more than one active voter registration record in Wisconsin. Other types of ERIC data are not readily available to WEC through other sources, such as data on registered Wisconsin voters who may have moved to and registered to vote in other states, who may have died in other states, and who may have voted multiple times in the same election.

WEC did not regularly obtain all types of data from ERIC in recent years.

As shown in Table 5, WEC did not regularly obtain all types of data from ERIC in recent years. From September 2016 to May 2021, WEC obtained some types of data every two years, but it obtained other types of data once during this period of time.

Table 5

ERIC Data that WEC Obtained, by Type[1]
As of July 2021

Type of Data	Sept. 2016	Sept. 2017	June 2018	Aug. 2019	Sept. 2019	May 2020	May 2021
Eligible residents who are not registered to vote	✓		✓			✓	
Registered voters who may have moved within Wisconsin, moved to and registered to vote in other states, or submitted new address information to the National Change of Address program		✓		✓			✓
Registered voters who may have voted multiple times in the same election					✓		
Registered voters who may have died in other states							✓
Registered voters who may have multiple voter registration records in Wisconsin							✓

[1] According to information provided by WEC's staff.

In August 2019, WEC obtained ERIC data on registered Wisconsin voters who may have moved within Wisconsin, who may have moved to and registered to vote in other states, or who submitted new address information to the National Change of Address program. It obtained these data for the time period from September 2017 through July 2019. These data included information on approximately 428,500 individuals, but WEC's staff eliminated duplicate and erroneous records, which left

information for 232,579 individuals in the data. In June 2019, WEC approved a plan for its staff to inactivate the voter registration records of all individuals whose voter registration status remained unresolved after the April 2021 Spring Election. In October 2019, WEC's staff sent letters to the 232,579 individuals, who were informed that they needed to confirm their current addresses or update their voter registration information.

As of August 2021, the voter registration records for:

- 153,156 of the 232,579 individuals (65.9 percent) remained active because, for example, the individuals had contacted their clerks, updated their records through the MyVote Wisconsin website, or had voted since October 2019;

- 69,196 individuals (29.8 percent) had been inactivated by WEC's staff because the individuals had not contacted their clerks and had not voted since October 2019; and

- 10,227 individuals (4.4 percent) had been inactivated for other reasons.

In May 2021, WEC obtained data on 743 registered Wisconsin voters who may have died in other states and data on approximately 16,000 registered voters who may have had multiple voter registration records in Wisconsin. It obtained these data for the time period from April 2018 through April 2021 and was still processing them at the time of our audit. Obtaining data on Wisconsin residents who may have died in other states is particularly important because DHS does not provide such information to WEC. Although DHS provides WEC with information about Wisconsin residents who died in the state, it cannot provide it with information about Wisconsin residents who died in other states because it and the health departments in all other states have agreed to share such information only with each other.

We contacted all five other midwestern states that are members of ERIC in order to determine how often they obtained ERIC data. Ohio did not respond, but:

- Illinois indicated that it regularly obtained all types of the available data, as required by its statutes, including some types as frequently as six times per year and other types as infrequently as once every two years;

- Iowa indicated that it annually obtained some types of the available data and planned to obtain all types of the available data each month beginning in 2022;

- Michigan indicated that it obtained some types of the available data every 18 months to 24 months; and

- Minnesota indicated that it obtained all types of the available data each month.

WEC's staff should work with WEC to establish a schedule for regularly obtaining each type of ERIC data.

ERIC data can help to ensure that Wisconsin's voter registration records are accurate and complete, as long as WEC obtains the data regularly and the data are acted upon before elections. WEC's staff should work with WEC to establish a schedule for regularly obtaining each type of data available from ERIC and a plan for acting on these data, including by deciding whether or not to inactivate relevant voter registration records. The schedule should allow sufficient time for WEC's staff and clerks to make such determinations before elections. In March 2021, WEC approved a schedule for obtaining each quarter the ERIC data on registered voters who may have moved within Wisconsin, who may have moved to and registered to vote in other states, or who submitted new address information to the National Change of Address program. These represent only one of the five types of data available from ERIC.

☑ Recommendation

We recommend staff of the Wisconsin Elections Commission:

- *work with the Wisconsin Elections Commission to establish a schedule for regularly obtaining each type of data available from the Electronic Registration Information Center and a plan for acting on these data; and*

- *report to the Joint Legislative Audit Committee by March 31, 2022, on their efforts to implement this recommendation.*

Issue for Legislative Consideration

The Legislature could consider modifying statutes to require WEC to regularly obtain ERIC data and use them to improve the accuracy and completeness of WisVote.

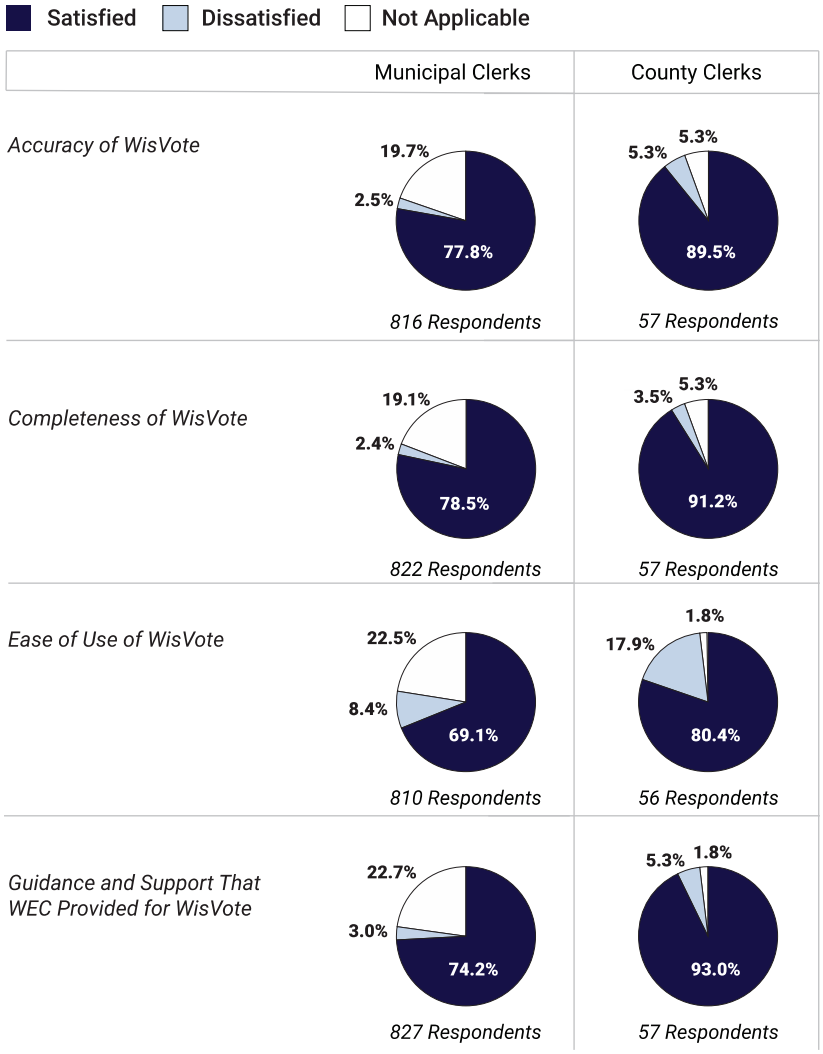
Currently, statutes do not require WEC to obtain and use ERIC data. The Legislature could consider modifying statutes to require WEC to regularly obtain ERIC data and use them to improve the accuracy and completeness of WisVote. For example, statutes could be modified to require WEC to regularly obtain every three or six months ERIC data for registered Wisconsin voters who may have moved to and registered to vote in other states, who may have voted in Wisconsin and other states, and who may have died in other states.

Satisfaction Levels of Clerks

Our April 2021 survey asked all municipal and county clerks about their satisfaction with WisVote. As shown in Figure 4, most of the municipal and county clerks who responded to our survey indicated that they were satisfied with the accuracy, completeness, and ease of use of WisVote, as well as with the guidance and support provided by WEC for using WisVote. County clerks indicated that they were more satisfied than municipal clerks with each of these aspects.

Figure 4

Satisfaction of Clerks with Aspects of WisVote[1]



[1]As indicated by municipal and county clerks who responded to our April 2021 survey.

Some clerks who responded to our survey commented on their satisfaction with WisVote. For example:

- one clerk indicated that WisVote is an "effective way to store and manage voter information;"
- a second clerk indicated that WisVote is a "wonderful, state of the art system;" and
- a third clerk indicated that WisVote is a "huge improvement" over SVRS, and that WEC's staff resolved problems "very quickly with thorough notice."

Other clerks who responded to our survey indicated their dissatisfaction with the accuracy of WisVote. For example:

- one clerk indicated that there have been data entry errors for many years; and
- a second clerk indicated that "a lot of the voter information," such as the birth dates of individuals who had registered to vote before Wisconsin had an electronic voter registration system, was inaccurate when first entered into SVRS and remains inaccurate in WisVote.

■ ■ ■ ■

Voting by Absentee Ballot
November 2020 General Election
Absentee Ballot Certificates
Collection of Absentee Ballots
Indefinitely Confined Individuals
Special Voting Deputies

Absentee Ballots

Statutes permit individuals to vote by absentee ballot.

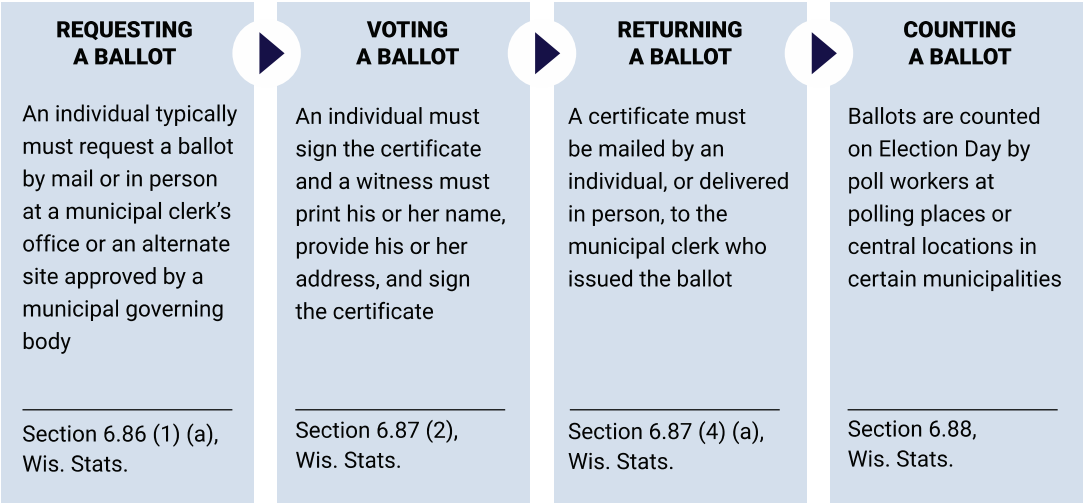
Statutes permit individuals to vote by absentee ballot. An individual must complete an absentee ballot in the presence of a witness and typically must complete a certificate that includes the addresses and signatures of the individual and a witness. In most instances, certificates are the envelopes in which absentee ballots are returned. To examine issues pertaining to absentee ballots cast in the November 2020 General Election, we examined WEC's data, contacted 48 clerks, and physically examined 14,710 certificates returned by individuals who voted in 29 municipalities. If WEC believes municipal clerks should be permitted to take certain actions pertaining to absentee ballots, we recommend WEC's staff work with WEC to promulgate applicable administrative rules. We also include five issues for legislative consideration.

Voting by Absentee Ballot

Figure 5 summarizes the typical process by which an individual votes by absentee ballot. Statutes typically require an individual to request an absentee ballot by mail or in person at either the office of a municipal clerk or alternate sites approved by municipal governing bodies. After receiving an absentee ballot and selecting candidates, statutes require an individual to sign the certificate and a witness to print his or her name, provide his or her address, and sign the certificate. Statutes require a certificate to be mailed by the individual, or delivered in person, to the municipal clerk who issued the absentee ballot. Absentee ballots are counted on Election Day by poll workers at polling places or central locations in certain municipalities.

Figure 5

Typical Process for Voting by Absentee Ballot, as Statutorily Required



When requesting absentee ballots, statutes require that individuals provide photo identification, unless individuals:

- are indefinitely confined because of age, physical illness, or infirmity, or they are disabled for indefinite periods of time;
- are residents of a residential care facility or qualified retirement home voting in the presence of special voting deputies;
- are serving in the military or vote overseas; or
- previously voted absentee, provided photo identification, and have not changed their names or addresses since then.

November 2020 General Election

Considerably more absentee ballots were cast in the November 2020 General Election than had been cast in the November 2016 General Election.

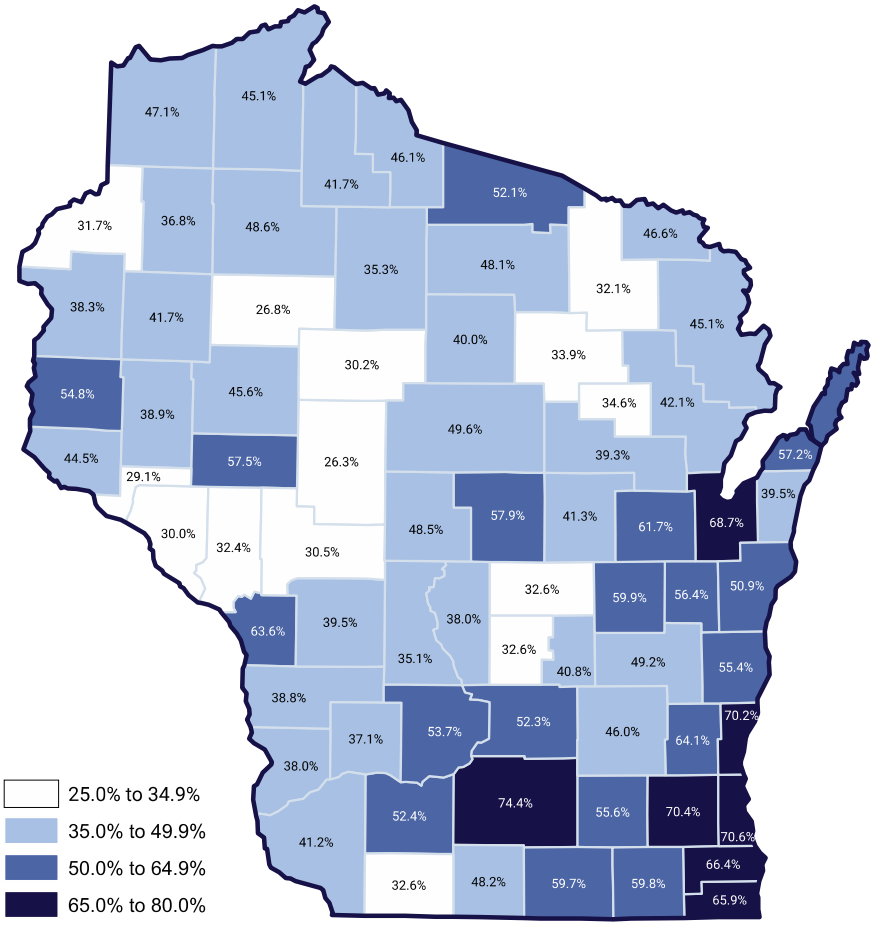
Considerably more absentee ballots were cast in the November 2020 General Election than had been cast in the November 2016 General Election. We found that:

- in November 2016, 819,316 absentee ballots were cast, which was 27.3 percent of all ballots cast; and
- in November 2020, 1,963,954 absentee ballots were cast, which was 59.6 percent of all ballots cast.

Figure 6 shows absentee ballots as a proportion of all ballots cast in each county in the November 2020 General Election. Dane County had the highest proportion of absentee ballots (74.4 percent), while Clark County had the lowest proportion (26.3 percent).

Figure 6

Absentee Ballots as a Proportion of All Ballots Cast, by County[1]
November 2020 General Election



[1] According to information in WisVote as of September 2021.

In February 2021, WEC used WisVote information to report that 4,270 of all absentee ballots in the November 2020 General Election (0.2 percent of all absentee ballots returned) were rejected. These ballots were rejected for a variety of reasons, including because the certificates were incomplete, the ballots were returned after Election Day, the individuals who cast the ballots died before Election Day, or

individuals voted in person at polling places on Election Day after having returned absentee ballots.

Absentee Ballot Certificates

Before providing an absentee ballot, statutes typically require a municipal clerk to verify that an individual provided valid identification. Statutes typically require an individual to complete an absentee ballot in the presence of an adult witness who is a U.S. citizen.

An absentee ballot certificate must include the signature of the individual who cast the ballot, and a witness must write his or her printed name, address, and signature.

Section 6.87 (2), Wis. Stats., requires a certificate to include the address and signature of the individual who cast the ballot, and it requires a witness to write his or her printed name, address, and signature on the certificate. Statutes do not specify which components, such as a street name and number, an address must include. Statutes include provisions pertaining to an improperly completed or incomplete certificate that an individual returns to a municipal clerk, including:

- s. 6.87 (9), Wis. Stats., which indicates that a clerk may return a ballot and its certificate if an individual is able to correct an improperly completed certificate and return the ballot in time for it to be counted on Election Day, but statutes do not otherwise permit or prohibit clerks from correcting errors in witness addresses or adding missing witness address information; and

- s. 6.87 (6d), Wis. Stats., which indicates that a ballot shall not be counted if its accompanying certificate does not have a witness address.

Section 5.01 (1), Wis. Stats., indicates that elections-related requirements should be construed to give effect to the will of electors, even when full compliance with some statutory provisions does not occur. Section 6.84 (2), Wis. Stats., indicates that notwithstanding s. 5.01 (1), Wis. Stats., the statutory provisions that require certificates to have witness addresses are mandatory, and the ballots accompanying certificates that are missing this information shall not be counted. Section 6.84 (2), Wis. Stats., similarly indicates that ballots accompanying certificates without voter or witness signatures shall not be counted during a recount.

In October 2016, WEC approved written guidance indicating that municipal clerks must take action to correct errors in the witness addresses on certificates.

In October 2016, WEC approved written guidance indicating that municipal clerks must take action to correct errors in the witness addresses on certificates. This guidance indicated that clerks were not required to contact the individuals who cast the ballots but were required to include their initials next to any corrections they made to witness addresses. This guidance also indicated that a complete address must include at least a street name and number as well as a municipality. In October 2020, WEC's staff updated this guidance to indicate that clerks should attempt to resolve any missing witness

address information before Election Day, and this can be done by using reliable information, such as personal knowledge, voter registration information, or a telephone call with a voter or witness. The guidance indicates that a witness does not need to appear in person to add a missing address. If certificates did not have signatures or contained other errors, the updated guidance indicated that clerks must require the individuals who cast the ballots or the witnesses to resolve these issues.

Our April 2021 survey asked municipal clerks whether they had received for the November 2020 General Election any certificates with missing information. In response, 507 clerks (58.9 percent) indicated that they had received certificates with missing information, 324 clerks (37.6 percent) indicated that they had not received such certificates, and 30 clerks (3.5 percent) indicated that they were uncertain whether they had received such certificates.

Municipal clerks indicated that they took various actions when they received certificates that did not have some or all components of witness addresses.

We contacted 21 municipal clerks about actions they took when they received certificates with missing information. All but one clerk indicated that they contacted the individuals who cast the ballots in order to allow them the opportunity to provide missing witness addresses. These clerks indicated that they took various actions when they received certificates that did not have some or all components of witness addresses. For example:

- 10 clerks indicated that they did not write any components of witness addresses on the certificates;
- 8 clerks indicated that they wrote components of witness addresses on the certificates;
- 2 clerks indicated that they accepted ballots returned in certificates that did not have any components of witness addresses; and
- 1 clerk indicated having rejected a certificate that did not have a witness address because the certificate was received the day before the election, which left too little time to obtain the missing address.

Statutes do not require municipal clerks to verify the signatures of individuals who cast absentee ballots. We reviewed information from 30 states where election officials verify signatures and found that ballot signatures are compared to signatures on other documents, such as absentee ballot applications, voter registration forms, and driver's licenses. Six of the 30 states specify criteria for verifying signatures, such as the writing slant, letter spacing, and letter shapes. In 28 of the 30 states, election officials notify individuals if their signatures are not verified, and 2 states require election officials to be trained to verify signatures. As noted, we found that WEC did not comply with statutes that require it to obtain from DOT the signatures of individuals who register online to vote.

Review of Certificates

To determine the extent to which the certificates of absentee ballots cast for the November 2020 General Election contained statutorily required information, we selected certificates in 29 municipalities, including:

- 9 of the 10 municipalities where the most absentee ballots were cast, other than the City of Madison, which did not allow us to physically handle certificates;
- the 10 municipalities where absentee ballots made up the largest proportions of the total ballots cast; and
- 10 municipalities we chose at random from counties other than those in which the other 19 municipalities were located.

The certificates we reviewed included spaces for individuals to sign their names, and for witnesses to write their addresses and signatures. The certificate that WEC made available to municipalities statewide to use in the November 2020 General Election did not include spaces for witnesses to print their names, as required by statutes.

We physically reviewed 14,710 certificates in 29 municipalities.

We physically reviewed 14,710 certificates in the 29 municipalities, where a total of 470,028 absentee ballots were cast in the November 2020 General Election. We reviewed a random sample of certificates from 20 municipalities, all or almost all certificates from 8 municipalities, and a large number of certificates from 1 municipality. Because of the size of our random sample of certificates that we reviewed in the 20 municipalities, we can reasonably expect that the results of our review for a given municipality are representative of all certificates in that municipality during the November 2020 General Election. However, because we did not examine certificates other than in the 29 municipalities, we cannot reasonably expect that the results of our review are representative of certificates in municipalities statewide. Appendix 4 lists the 29 municipalities and selected results of our review of certificates.

Our review found that some certificates had incomplete witness addresses or did not have some statutorily required information.

Our review of the 14,710 certificates found that:

- 1,022 certificates (6.9 percent) in 28 municipalities had partial witness addresses because they did not have one or more components of a witness address, such as a street name, municipality, state, and zip code, including 799 certificates (5.4 percent) that did not have a zip code and 364 certificates (2.5 percent) that did not have a state;

- 15 certificates (0.1 percent) in 10 municipalities did not have a witness address in its entirety;
- 8 certificates (less than 0.1 percent) in 7 municipalities did not have a witness signature; and
- 3 certificates (less than 0.1 percent) in 2 municipalities did not have a voter's signature.

Our review of the 14,710 certificates found evidence that municipal clerks had corrected witness addresses on 66 certificates (0.4 percent). This evidence included clerk initials or pen marks in the ink colors that clerks had indicated were used to make corrections. As noted, WEC's written guidance in October 2016 indicated that clerks must include their initials next to any corrections to witness addresses.

On Election Day, poll workers remove the returned ballots from certificates, which are retained separately from the ballots. As a result, almost all certificates we reviewed no longer contained ballots. However, we found 17 certificates in 3 of the 29 municipalities contained absentee ballots. Clerks in these three municipalities indicated that the corresponding ballots were likely not counted on Election Day because of oversights. Most of these 17 certificates were not in the 14,710 certificates in our sample.

We question whether clerks in four municipalities consistently complied with the statutory requirement for them to initial certificates in certain situations.

Statutes require municipal clerks to write their initials on certificates in certain situations, including when individuals request absentee ballots in person at clerk offices. These initials indicate that clerks verified the identification provided by these individuals when they requested absentee ballots. Statutes indicate that a ballot must not be counted if the accompanying certificate is not initialed by a clerk, when such initials are required. In contrast, statutes do not require clerks to write their initials on certificates accompanying absentee ballots requested online by individuals. Such individuals are statutorily required to provide clerks with a copy of their photo identification. During our review of the 14,710 certificates, we found that less than 1.0 percent of all certificates we reviewed in four municipalities contained clerk initials. Clerks at these municipalities indicated that they did not initial certificates for multiple reasons, including because the individuals who requested the ballots were registered and eligible to receive them; the clerks printed the names and addresses of the individuals on the certificates to signify the individuals were eligible to receive the ballots; and the clerks initialed the ballots rather than the certificates. We question whether the clerks in these four municipalities consistently complied with the statutory requirement for them to initial certificates in certain situations.

Election Day Forms

Statutes require poll workers to complete a form that contains certain information.

Statutes require poll workers to complete a form that contains certain information, including the number of individuals on the poll list and the number of ballots returned. These forms also contain incident logs, where poll workers can describe election-related occurrences at polling places, such as ballots remade by workers and absentee ballots rejected by poll workers. County clerks typically retain these forms after an election.

We selected a random sample of 319 municipalities and requested that the relevant county clerks provide us with all forms that poll workers in these municipalities completed on Election Day in November 2020 at polling places other than central count locations, which is where some municipalities specify that all absentee ballots are counted on Election Day. The 319 municipalities are located in 69 counties and listed in Appendix 5. We received forms for all 319 municipalities.

In the 319 municipalities in our review, the forms we reviewed indicated that 2,187 ballots (0.6 percent) were remade and 231 absentee ballots (less than 0.1 percent) were rejected.

Poll workers are required by statutes to remake ballots if, for example, the electronic voting equipment cannot read ballots in poor condition, individuals select more candidates than allowed in a given contest, or individuals who are in the military or overseas return electronic ballots. When a ballot is remade, poll workers are statutorily required to complete a new ballot that reflects the choices made on the original ballot. Poll workers may reject absentee ballots if, for example, the accompanying certificates are incomplete or the voters who returned them died before Election Day. The 571 forms we reviewed indicated that a total of 392,177 ballots were cast in the 319 municipalities, including:

- 2,187 ballots (0.6 percent) remade in 146 municipalities; and
- 231 absentee ballots (less than 0.1 percent) rejected in 78 municipalities.

Improved Procedures

WEC's staff should work with WEC to ensure the certificates made available to municipalities comply with statutes by requiring witnesses to print their names, which will allow municipal clerks to more readily identify the witnesses. WEC's staff should provide municipal clerks with additional training on the statutory requirement to initial certificates in certain situations. If WEC believes that clerks should be permitted to correct or add missing witness addresses on certificates, WEC's staff should work with WEC to promulgate administrative rules to permit clerks to take such actions. Promulgating administrative rules allows the Governor and the Legislature to participate in the process of determining how clerks are to act when they receive certificates that do not have statutorily required information, and administrative rules carry the force of law.

☑ Recommendation

We recommend staff of the Wisconsin Elections Commission:

- *ensure that the absentee ballot certificates made available to municipalities comply with statutes by requiring witnesses to print their names;*
- *provide municipal clerks with additional training on the statutory requirement to initial absentee ballot certificates in certain situations;*
- *promulgate administrative rules to allow municipal clerks to correct or add missing witness address information to absentee ballot certificates, if the Wisconsin Elections Commission believes municipal clerks should be permitted to take such actions; and*
- *report to the Joint Legislative Audit Committee by March 31, 2022, on their efforts to implement these recommendations.*

Issues for Legislative Consideration

The Legislature could consider modifying statutes to specify the particular address components that a witness must provide on a certificate.

As noted, statutes do not define the components of a witness address that a certificate must contain, such as a street name and number, municipality, state, and zip code. The Legislature could consider modifying statutes to specify the particular address components that a witness must provide on a certificate. For example, witnesses could be required to provide, at a minimum, street names and numbers, as well as their municipalities. Such a definition would allow an absentee ballot to be counted if a witness address excluded a state and a zip code.

The Legislature could consider modifying statutes to clarify whether municipal clerks themselves can correct errors in witness addresses or add missing witness address information.

The Legislature could consider modifying statutes to clarify the extent to which municipal clerks are permitted themselves to correct errors in witness addresses or add missing witness address information. As noted, statutes allow a clerk to return a ballot and its certificate if an individual is able to correct an improperly completed certificate and return the ballot in time for it to be counted on Election Day, but statutes do not otherwise permit or prohibit clerks from correcting errors in witness addresses or adding missing witness address information.

The Legislature could consider modifying statutes to require municipal clerks to verify the signatures of individuals who cast absentee ballots.

As noted, statutes require a certificate to include the signature of the individual who cast the ballot. The Legislature could consider modifying statutes to require municipal clerks to verify the signatures of individuals who cast absentee ballots. In doing so, it could specify the documents that clerks should use to verify these signatures, such as voter registration forms and driver's licenses, and the methods that clerks should use to verify these signatures, such as examining the writing slant, letter spacing, and letter shapes. In addition, it could require clerks to be trained on how to verify signatures.

Collection of Absentee Ballots

Statutes require a certificate to be mailed by the individual, or delivered in person, to the municipal clerk who issued the ballot.

As noted, statutes require a certificate to be mailed by the individual, or delivered in person, to the municipal clerk who issued the ballot. Statutes allow a municipal governing body to designate a site other than a municipal clerk's office as the location where individuals may request, vote, and return absentee ballots for a given election. If such a site is designated, no functions related to voting and returning absentee ballots that are conducted at such a site may be conducted at a clerk's office. Statutes do not permit or prohibit ballot drop boxes.

In March 2020, WEC's staff issued written guidance indicating that municipal clerks can allow individuals to return absentee ballots to drop boxes that are secure, monitored, and emptied regularly, or return the ballots through mail slots at municipal facilities and book return slots at municipal libraries, as long as clerks collected such ballots daily. In July 2020, WEC's staff issued written guidance indicating that alternate sites for requesting, voting, and returning absentee ballots could be established according to the statutory requirements.

Drop Boxes

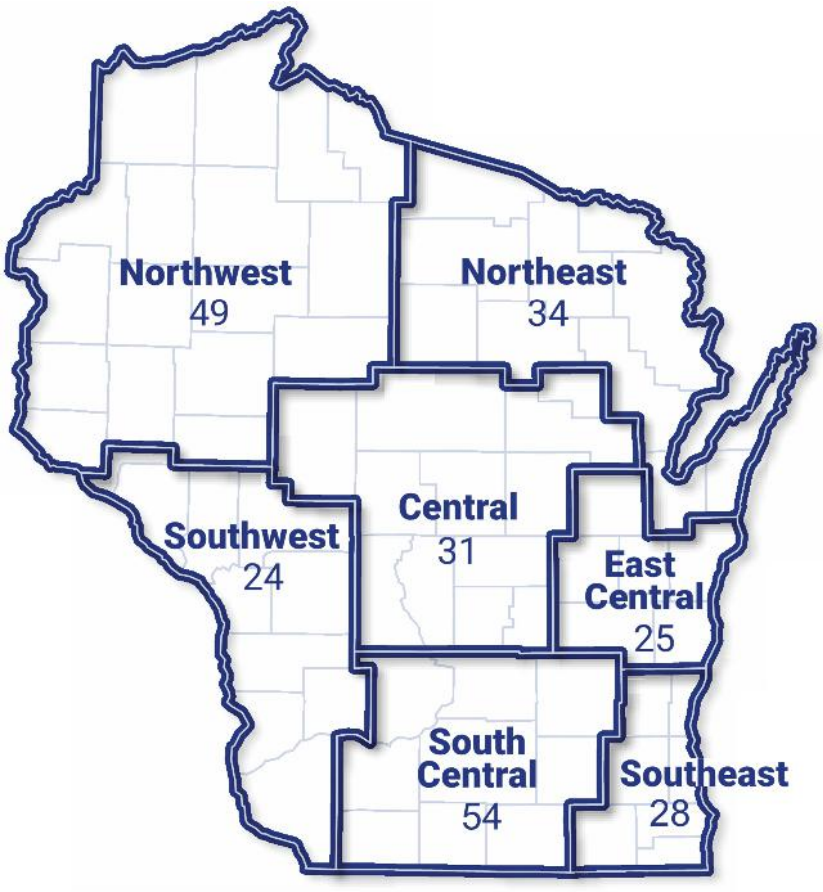
In response to our survey, 245 municipal clerks indicated that they used drop boxes for the November 2020 General Election.

Our survey asked municipal clerks to indicate whether they used drop boxes, other than mail slots at municipal facilities, to collect absentee ballots for the November 2020 General Election. In response to our survey:

- 610 clerks (71.3 percent) indicated that they did not use drop boxes; and
- 245 clerks (28.7 percent) indicated that they used drop boxes, and the municipalities of these clerks were located throughout the state, as shown in Figure 7.

Figure 7

Number of Municipalities That Used Ballot Drop Boxes, by Region[1]
November 2020 General Election



[1] As indicated by 245 municipal clerks who responded to our April 2021 survey.

A total of 26 of the 47 municipal clerks we contacted indicated that they used drop boxes, municipal return slots, or similar receptacles for the November 2020 General Election. We found that:

- 25 clerks indicated that absentee ballots were collected from drop boxes at least daily, and 1 clerk indicated that ballots were collected three times per week from a drop box that was locked and under surveillance;
- 25 clerks indicated that their drop boxes were locked or had tamper-evident seals; and
- 14 clerks indicated that they used camera or local law enforcement surveillance to monitor their drop boxes.

Information from the National Conference of State Legislatures (NCSL) indicates that 11 states, which are listed in Appendix 9, allowed drop boxes as of September 2020. In June 2021, a law firm asked the Waukesha County Circuit Court for a declaratory judgement that statutes do not allow drop boxes. As of September 2021, the court had not issued its decision.

If WEC believes that municipal clerks should be permitted to establish drop boxes where individuals can return absentee ballots, WEC's staff should work with WEC to promulgate administrative rules to permit clerks to establish them. Such rules could establish minimum requirements for securing the drop boxes, as well as prescribe where clerks could locate drop boxes and how frequently clerks would be required to collect absentee ballots from drop boxes. Promulgating administrative rules allows the Governor and the Legislature to participate in the process of determining how individuals can return absentee ballots, and administrative rules carry the force of law.

☑ Recommendation

We recommend staff of the Wisconsin Elections Commission:

- *promulgate administrative rules to permit municipal clerks to establish drop boxes where individuals can return absentee ballots, if the Wisconsin Elections Commission believes municipal clerks should be permitted to establish drop boxes; and*

- *report to the Joint Legislative Audit Committee by March 31, 2022, on their efforts to implement this recommendation.*

Special Events

Media reports indicated that at least one clerk collected absentee ballots at specified outdoor locations before the November 2020 General Election. Our survey asked municipal clerks to indicate whether they had held events at sites other than their offices to collect absentee ballots for the General Election. In response:

- 842 clerks (98.5 percent) indicated that they had not held such events; and

- 13 clerks (1.5 percent) indicated that they had held such events.

We contacted 11 municipal clerks about events at sites other than their offices to collect absentee ballots. Some clerks, particularly in smaller municipalities, indicated that they did not have offices in municipal buildings and performed election-related duties in their homes. To minimize the number of individuals in their homes during the public

health emergency, some clerks indicated that they had conducted in-person absentee voting at locations other than their homes. None of the 11 clerks indicated that their municipal governing bodies had designated alternate sites for in-person absentee voting. Among the 11 clerks:

- 7 clerks indicated that they had held special events at sites other than their offices, and individuals could return absentee ballots at these events;
- 4 clerks indicated that they had held special events at sites other than their offices, and individuals could both request and return absentee ballots at these events;
- 1 clerk indicated having conducted in-person absentee voting at the clerk's home, which was not the clerk's office; and
- 1 clerk indicated having conducted in-person absentee voting by visiting the homes of individuals who requested ballots.

Issue for Legislative Consideration

The Legislature could consider modifying statutes to clarify whether individuals are allowed to return absentee ballots to drop boxes.

The Legislature could consider modifying statutes to clarify whether individuals are allowed to return absentee ballots to drop boxes. Some individuals believe that statutes allow absentee ballots to be returned to drop boxes or in person to clerk staff at locations other than a clerk's office, regardless of whether a municipal governing body established such locations. They believe that these actions are statutorily allowable because individuals requested ballots by statutorily allowable methods, the drop boxes were established by clerks, and clerk staff collected the ballots. Other individuals believe that statutes do not allow absentee ballots to be returned through drop boxes or to clerk staff at locations other than those designated by a municipal governing body.

Indefinitely Confined Individuals

Statutes allow individuals to sign statements indicating they are indefinitely confined because of age, physical illness, or infirmity.

Statutes allow individuals to sign statements indicating they are indefinitely confined because of age, physical illness, or infirmity, or because they are disabled for an indefinite period. Such individuals are not required to provide proof of their identification in order to receive absentee ballots. Instead, statutes allow them to submit signed statements from witnesses who observed them voting their ballots. These statements must contain the names and addresses of the individuals and verify the accuracy of this information.

The Wisconsin Supreme Court ruled that individuals must decide, based on their age, physical illness, or infirmity, whether they are indefinitely confined.

In March 2020, WEC provided guidance to municipal clerks indicating that indefinitely confined designations are determined by individuals and are based on their circumstances, do not require permanent or total inability to travel outside of the home, and should not be used in order to avoid providing photo identification for voting. On December 14, 2020, the Wisconsin Supreme Court ruled that individuals must decide, based on their age, physical illness, or infirmity, whether they are indefinitely confined.

Statutes require municipal clerks to automatically send absentee ballots to all indefinitely confined individuals unless:

- an individual does not cast and return an absentee ballot for a given election and does not respond within 30 days to a letter or a postcard mailed by a clerk;
- an individual requests to no longer be considered to be indefinitely confined; or
- a clerk receives reliable information that an individual is no longer indefinitely confined.

In the November 2020 General Election, 220,404 indefinitely confined individuals voted, including 169,901 individuals who first indicated in 2020 that they were indefinitely confined.

As shown in Table 6, 220,404 indefinitely confined individuals voted in the November 2020 General Election, including 169,901 individuals (77.1 percent) who first indicated in 2020 that they were indefinitely confined. We found that 1,001 individuals first indicated for the November 2020 General Election that they were indefinitely confined but, in fact, voted at the polls on November 3, 2020. Because these individuals were not indefinitely confined on Election Day, they are not included in the table.

Table 6

Indefinitely Confined Individuals Who Voted in the November 2020 General Election, by the Year When They First Indicated They Were Indefinitely Confined[1]

Year	Number of Individuals	Percentage of Total
Before 2016	16,573	7.5%
2016	12,658	5.7
2017	2,928	1.3
2018	13,840	6.3
2019	4,504	2.0
2020	169,901	77.1
Total	**220,404**	**100.0%**

[1] According to WEC's data.

A total of 171,850 of the 220,404 indefinitely confined individuals (78.0 percent) had previously provided photo identification.

WEC's data indicated that 171,850 of the 220,404 indefinitely confined individuals (78.0 percent) had previously provided photo identification. According to WEC's data, the remaining 48,554 individuals (22.0 percent) had not previously voted by methods that required them to have provided photo identification or did not have photo identifications on file with clerks. These data indicated the locations from which 44,272 of the 48,554 individuals (91.2 percent) voted during the November 2020 General Election. We found that these individuals voted from each county in the state, as shown in Appendix 10.

Our survey asked municipal clerks to indicate whether they had sent absentee ballots to indefinitely confined individuals for the November 2020 General Election. In response to our survey:

- 829 clerks (95.6 percent) indicated that they had sent absentee ballots to indefinitely confined individuals;
- 36 clerks (4.2 percent) indicated that they had not sent ballots to such individuals; and
- 2 clerks (0.2 percent) indicated that they were uncertain whether they had sent ballots to such individuals.

We contacted seven municipal clerks regarding their perspectives on indefinite confinement and found that:

- four clerks indicated they had contacted individuals to verify their indefinitely confined status;
- two clerks indicated certain individuals who claimed indefinite confinement status did not meet the requirement, but they did not contact these individuals before sending them absentee ballots; and
- one clerk indicated postcards were not mailed to indefinitely confined individuals who had not returned absentee ballots in prior elections and, as a result, these individuals automatically received absentee ballots for the November 2020 General Election.

Information from NCSL indicated that nine other states, which are listed in Appendix 11, allow individuals with certain disabilities to automatically receive absentee ballots. Some states require physicians to verify that certain individuals are eligible to automatically receive absentee ballots, and states use various methods to determine when individuals are no longer eligible.

Special Voting Deputies

Statutes set forth the exclusive means of absentee voting in person in residential care facilities and qualified retirement homes.

Statutes set forth the exclusive means of absentee voting in person in residential care facilities and qualified retirement homes. A municipal clerk must appoint at least two special voting deputies to supervise absentee voting by individuals living in such facilities and homes, a clerk is required to send deputies to each such facility and home where five or more individuals live and are registered to vote, and deputies must arrange one or more visits to each such facility and home. Instead of providing proof of identification, individuals may submit statements that verify their names and addresses, and both deputies must sign the statements. The individuals must vote in the presence of the deputies. A clerk may send an absentee ballot to an individual who is unable to vote during two separate visits by the deputies.

In March 2020, WEC's staff issued written guidance indicating that municipal clerks should not send special voting deputies to facilities and homes but should instead mail absentee ballots to individuals living in such facilities and homes. WEC's staff did so based on WEC's interpretation that the deputies were "non-essential" individuals prohibited from visiting facilities and homes as a result of Executive Order 72 and DHS directives pertaining to the public health emergency. In May 2020, the Wisconsin Supreme Court blocked an extension of DHS's "Safer at Home" directive.

Written guidance that WEC provided to municipal clerks in June 2020 did not comply with statutes.

In June 2020, WEC's staff recommended to WEC a motion to direct municipal clerks to contact facilities and homes in order to determine if special voting deputies would be permitted entry. In June 2020, WEC directed clerks not to send or attempt to send deputies to facilities and homes for the remainder of 2020. Instead, WEC directed clerks to mail absentee ballots to individuals living in these facilities and homes who requested the ballots. WEC's written guidance provided to clerks in June 2020, as well as the written guidance that WEC's staff had provided to clerks in March 2020, did not comply with statutes.

Our survey asked municipal clerks to indicate whether they tried to send special voting deputies to facilities or homes before the November 2020 General Election. In response to our survey:

- 502 clerks (58.8 percent) indicated that they did not have such facilities or homes in their municipalities;
- 342 clerks (40.0 percent) indicated that they had not tried to send deputies to such facilities and homes; and
- 10 clerks (1.2 percent) indicated that they had attempted to send deputies to such facilities and homes.

We contacted nine municipal clerks about whether they had attempted to send special voting deputies to facilities or homes before the November 2020 General Election. Seven clerks told us that they had contacted facilities and homes, none of which permitted the deputies to enter, and two of these seven clerks indicated that staff of the facilities and homes helped individuals living there to complete absentee ballots.

In February 2021, the Joint Committee for Review of Administrative Rules determined that WEC's written guidance to municipal clerks not to send special voting deputies to facilities and homes but to instead mail absentee ballots to individuals living there met the definition of a rule. As a result, the Joint Committee directed WEC to promulgate an emergency rule within 30 days. In March 2021, WEC issued new written guidance that directed clerks to contact facilities and homes before the April 2021 Spring Election and determine if deputies would be permitted entry, schedule two televisits with administrators of facilities and homes where deputies would not be permitted entry, and mail absentee ballots to individuals living in such facilities and homes. WEC also directed its staff to create a scope statement for a proposed emergency rule based on the March 2021 guidance. In April 2021, WEC passed a motion to allow this scope statement to expire, in part, because no further statewide elections were scheduled to occur in 2021.

Improved Procedures

If WEC believes clerks should be permitted in certain situations not to send special voting deputies to residential care facilities and qualified retirement homes, WEC's staff should work with WEC to promulgate administrative rules to permit clerks to take alternative actions. Promulgating administrative rules allows the Governor and the Legislature to participate in the process of determining how clerks are to provide absentee ballots to individuals living in such facilities and homes, and administrative rules carry the force of law.

☑ Recommendation

We recommend staff of the Wisconsin Elections Commission:

- *promulgate administrative rules to specify the situations when municipal clerks should not send special voting deputies to residential care facilities and qualified retirement homes, if the Wisconsin Elections Commission believes municipal clerks should be permitted to take alternative actions in these situations; and*

- *report to the Joint Legislative Audit Committee by March 31, 2022, on their efforts to implement these recommendations.*

Issue for Legislative Consideration

The Legislature could consider modifying statutes to prescribe circumstances when clerks are not required to send special voting deputies to facilities and homes.

Currently, statutes require municipal clerks to attempt to send special voting deputies to residential care facilities and qualified retirement homes, regardless of the circumstances. During a public health or other emergency, clerks and special voting deputies may risk disenfranchising individuals living in such facilities and homes if they cannot obtain entry. The Legislature could consider modifying statutes to prescribe circumstances when clerks are not required to send special voting deputies to such facilities and homes, as well as the procedures clerks must follow in mailing and considering absentee ballots in such circumstances. In September 2021, WEC voted to request that the Governor categorize special voting deputies as essential visitors, which it indicated would allow the deputies entry into facilities and homes during a public health emergency.

■ ■ ■ ■

Ballot Processing

Statutes permit a municipal governing body to specify by ordinance that absentee ballots returned by individuals will be counted on Election Day at a central location.

Statutes permit a municipal governing body to specify by ordinance that absentee ballots returned by individuals will be counted on Election Day at a central location, rather than at each polling place. A municipal clerk, or an election official designated by a municipal or county clerk, must direct all central count proceedings, including counting ballots publicly. During the November 2020 General Election, 39 municipalities counted absentee ballots at central count locations. We contacted the clerks of all 39 municipalities and analyzed the written guidance WEC and its staff provided to clerks. We recommend WEC's staff work with WEC to retract statutorily noncompliant written guidance previously provided to municipal clerks, and WEC's staff should work with WEC to promulgate administrative rules if WEC believes clerks should be permitted to take certain actions. We also include two issues for legislative consideration.

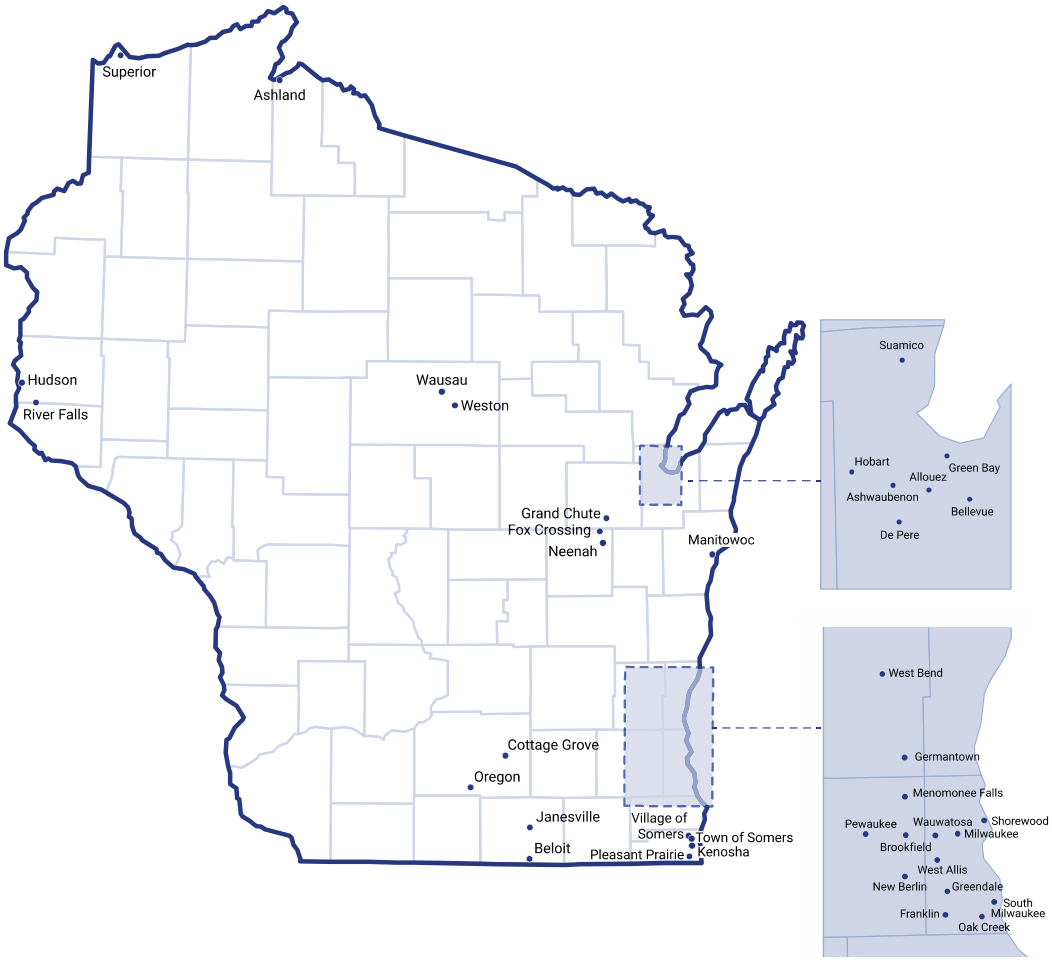
Central Count Locations

During the November 2020 General Election, 39 municipalities used central count locations.

Figure 8 shows the 39 municipalities that used central count locations during the November 2020 General Election. Municipal clerks indicated that 32 of the 39 municipalities authorized central count locations in 2016 or later, including 8 municipalities that authorized them in 2020.

Figure 8

Municipalities That Used Central Count Locations
November 2020 General Election



Election Day Forms

For the 39 municipalities that used central count locations, we reviewed 662 Election Day forms that poll workers completed for the November 2020 General Election for their central count locations. As noted, poll workers are required by statutes to remake ballots if, for example, the electronic voting equipment cannot read ballots in poor condition, individuals select more candidates than allowed in a given contest, or individuals who are in the military or overseas return electronic ballots. Absentee ballots may also be rejected on Election Day if, for example, the accompanying certificates are incomplete.

For the November 2020 General Election, 12,237 absentee ballots (1.4 percent) were remade in the 39 central count municipalities.

The 662 Election Day forms indicated that 12,237 ballots were remade at central count locations in the 39 municipalities during the November 2020 General Election, which was approximately 1.4 percent of all ballots cast in these municipalities. This proportion was higher than the 0.6 percent of all ballots remade in our sample of 319 municipalities. This higher proportion may be explained, in part, because individuals who vote in person at polling places are allowed to spoil their ballots and recast them, whereas poll workers at central count facilities processed only absentee ballots.

Central count poll workers in 2 municipalities remade considerably larger proportions of ballots than poll workers in the other 37 municipalities. We found that central count poll workers in the:

- Town of Grand Chute in Outagamie County remade 2,249 absentee ballots, which was approximately 16.3 percent of all ballots cast in the municipality. The Outagamie County clerk indicated to WEC's staff that they had encountered an issue when printing absentee ballots, which caused the ballots to be completely unreadable when inserted into electronic voting equipment. As a result, poll workers remade the ballots.

- City of West Bend remade 1,881 absentee ballots, which was approximately 10.3 percent of all ballots cast in the municipality. The municipal clerk indicated to us that creases in the absentee ballots caused the electronic voting equipment to register over-votes, which occur when a ballot includes more votes than allowed for a given contest. As a result of these over-votes, poll workers remade the ballots.

For the November 2020 General Election, 633 absentee ballots (less than 0.1 percent) were rejected in 33 of the 39 central count municipalities.

The 662 Election Day forms indicated that 633 absentee ballots were rejected at central count locations in 33 of the 39 municipalities during the November 2020 General Election, which was less than 0.1 percent of the total ballots cast in these 33 municipalities. This proportion was similar to the proportion that poll workers rejected in our previously described sample of 319 municipalities.

Ballot Security

Municipal clerks indicated that central count locations used a variety of security measures on Election Day. A total of 23 municipal clerks indicated that cameras, locked doors, and vaults provided security. In addition, 30 clerks indicated either that law enforcement officers had offices at or patrolled the central count locations, or that these locations were in municipal halls, which the clerks believed increased the level of security.

Absentee ballots returned by individuals are stored in the offices of municipal clerks before Election Day. Absentee ballots must be transported to a central count location on Election Day if such a location is separate from a clerk's office. Thirteen of the 39 municipal clerks indicated that the central count locations in November 2020 were separate from their municipal halls, although all 13 clerks indicated that these locations were within 15 minutes of travel time from their offices. Among the 13 clerks:

- 6 clerks indicated that they transported the absentee ballots to the central count locations;
- 6 clerks indicated that their staff, municipal employees, or poll workers transported the ballots; and
- 1 clerk indicated that law enforcement officers transported the ballots.

Poll Workers

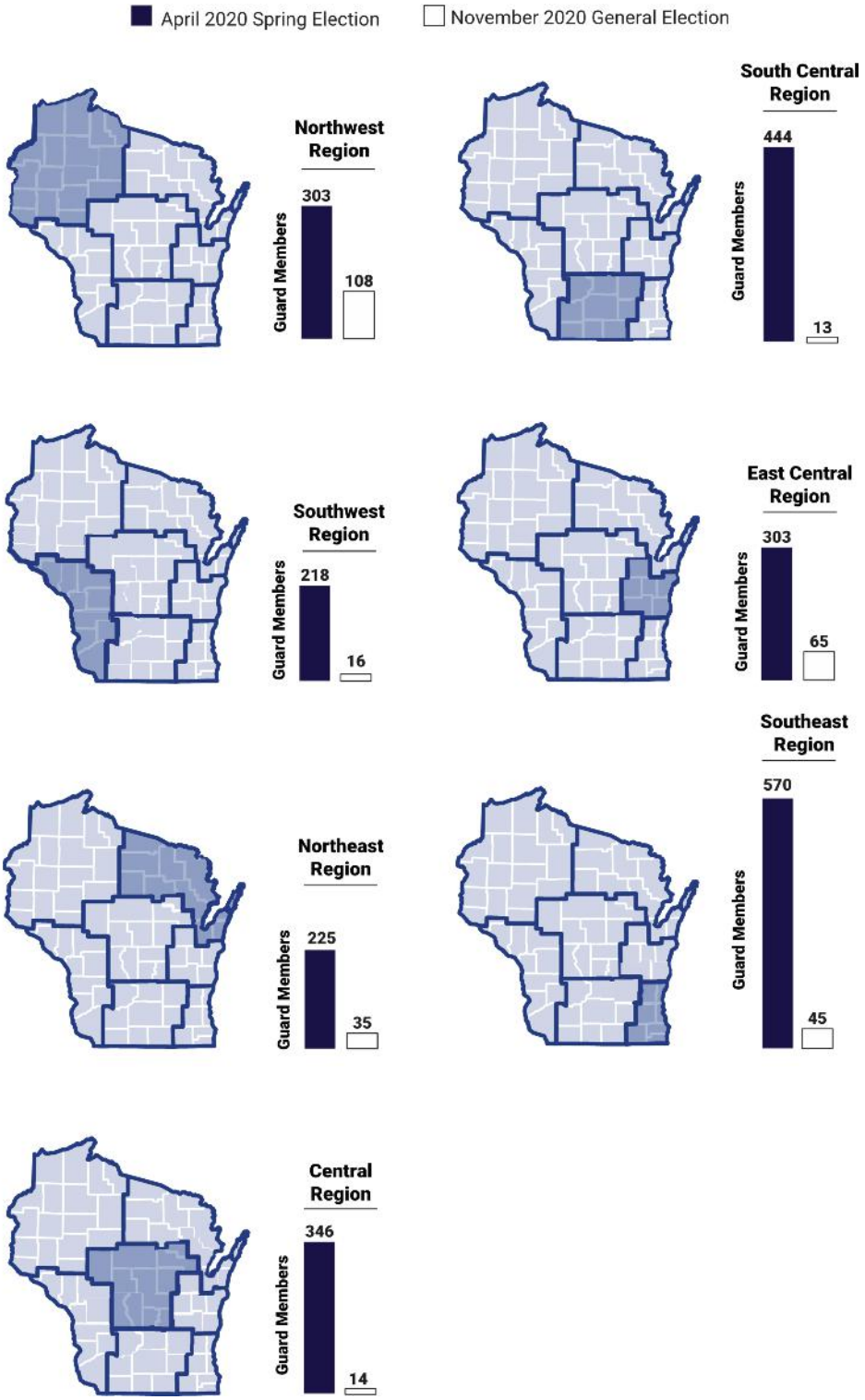
Statutes require at least five poll workers to serve at each polling place. Poll workers maintain order, ensure that ballot boxes and poll lists are secure, and ensure that electronic voting equipment works properly. To help address poll worker shortages in 2020, WEC requested assistance from the National Guard.

During four elections and primaries in 2020, 3,482 National Guard members worked at polling places in 71 counties.

Data provided by WEC's staff indicated that a total of 3,482 National Guard members worked at polling places in 71 counties during four elections and primaries from April 2020 through November 2020, including 2,409 members in April 2020 and 296 members in November 2020. A given member may have worked at multiple elections. Figure 9 shows the number of National Guard members who worked in each of seven regions in the April 2020 Spring Election and in the November 2020 General Election.

Figure 9

National Guard Members Who Worked at Polling Places, by Region[1]
April 2020 Spring Election and November 2020 General Election



[1] According to data provided by WEC's staff.

Statutes permit certain individuals other than poll workers to be present at polling places and central count locations. For example, a municipal governing body may authorize a municipal clerk to employ individuals to help count ballots, and trained technicians needed to operate automatic tabulating equipment may be present at central count locations. All proceedings at a central count location must be open to the public, but no individual other than those employed and authorized may touch any ballot, certificate, or electronic voting equipment. Statutes do not specify the actions and responsibilities that consultants are allowed to take at polling places and central count locations on Election Day.

Consultants associated with non-profit organizations worked at the central count locations in 2 of the 39 municipalities during the November 2020 General Election.

We asked the clerks of all 39 municipalities whether consultants worked at central count locations during the November 2020 General Election. Clerks indicated that consultants associated with non-profit organizations worked at the central count locations in 2 of the 39 municipalities. Specifically:

- One municipality indicated that a consultant attended the August 2020 primary as an observer, helped to modify the municipality's election training materials from August 2020 until October 2020, and was at the central count location on Election Day in November 2020 to provide technical assistance for electronic voting equipment. The municipality indicated that at least five poll workers monitored such assistance at all times.

- A second municipality indicated that a consultant provided logistical support and offered elections administration recommendations but did not have the authority to make decisions and did not count ballots. The municipality indicated that the consultant initially wore a city employee identification badge at the central count location on Election Day in November 2020 but subsequently became an observer after the deputy clerk spoke with WEC's administrator about this individual.

Issue for Legislative Consideration

The Legislature could consider modifying statutes to specify the actions and responsibilities for consultants at polling places and central count locations on Election Day.

The Legislature could consider modifying statutes to specify the actions and responsibilities for consultants at polling places and central count locations on Election Day. For example, statutes could specify the particular actions that consultants are permitted to take, as well as the responsibilities that they are allowed to assume while helping municipal clerks to administer elections.

Ballot Counting

Statutes require election officials to count ballots without adjourning until the counting is completed.

Regardless of whether a municipality uses a central count location, statutes require election officials to count ballots without adjourning until the counting is completed. Within two hours of completing such counting on Election Night, municipalities must report the results to the relevant county clerks.

Written guidance that WEC's staff provided to municipal clerks in October 2020 did not comply with statutes.

Because of the increased number of absentee ballots submitted in 2020, municipal clerks expressed concerns about their ability to count ballots without adjourning. In March 2020, WEC's staff issued written guidance indicating that clerks unable to count all absentee ballots on Election Day could reconvene the following morning. In April 2020, the U.S. Supreme Court ruled that all absentee ballots postmarked by Election Day for the Spring Election were valid, even if clerks did not receive them until after Election Day. In October 2020, WEC's staff issued written guidance indicating that although statutes do not permit adjourning while counting ballots and that clerks should complete all required tasks before adjourning on Election Night, inevitable circumstances may occur that require adjourning until the following day. This written guidance did not comply with statutes.

None of the clerks of the 39 municipalities with central count locations indicated to us that they had adjourned before having counted all ballots after the polls closed for the November 2020 General Election. Nevertheless, the potential exists that clerks could adjourn from counting ballots in future elections, based on written guidance from WEC's staff.

WEC's staff should retract their statutorily noncompliant written guidance indicating that although clerks should complete all required tasks before adjourning on Election Night, inevitable circumstances may occur that require adjourning until the following day. If WEC believes certain circumstances may justify adjourning before ballot counting is completed, WEC's staff should work with WEC to promulgate administrative rules to permit adjourning. Promulgating administrative rules allows the Governor and the Legislature to participate in the process of determining how clerks are to count ballots, and administrative rules carry the force of law.

☑ Recommendation

We recommend staff of the Wisconsin Elections Commission:

- *retract their statutorily noncompliant written guidance that indicates municipal clerks may adjourn before counting all ballots as a result of inevitable circumstances;*

- *promulgate administrative rules to allow municipal clerks to adjourn in certain circumstances before*

completing ballot counting, if the Wisconsin Elections Commission believes municipal clerks should be allowed to adjourn in these circumstances; and

- *report to the Joint Legislative Audit Committee by March 31, 2022, on its efforts to implement these recommendations.*

Polling Places

Statutes require a municipal governing body to establish polling places at least 30 days before an election.

Statutes require a municipal governing body to establish polling places at least 30 days before an election. In March 2020, the Governor issued Executive Order 72, which directed DHS to take all necessary and appropriate measures to respond to the public health emergency. DHS subsequently issued directives that barred nonessential individuals from visiting nursing homes and other licensed care facilities, where polling places are often located.

Written guidance that WEC provided to municipal clerks in March 2020 did not comply with statutes.

In March 2020, WEC approved written guidance indicating that municipal clerks can relocate polling places without approval from municipal governing bodies. Because Executive Order 72 had been issued less than 30 days before the April 2020 election, WEC's staff indicated that clerks needed the flexibility to quickly establish new polling places and ensure that individuals were not disenfranchised because nursing homes and licensed care facilities were closed to the public. As of August 2021, WEC had not retracted or modified its written guidance, even though municipal governing bodies have had the opportunity since March 2020 to establish new polling places that are open to the public.

WEC's staff should work with WEC to retract the statutorily noncompliant written guidance that indicates municipal clerks can relocate polling places without approval from municipal governing bodies. If WEC believes that certain circumstances may justify permitting clerks to relocate polling places without approval, such as during a public health or other emergency, WEC's staff should work with WEC to promulgate administrative rules to permit quick relocations. Promulgating administrative rules allows the Governor and the Legislature to participate in the process of determining how polling places are located, and administrative rules carry the force of law.

☑ Recommendation

We recommend staff of the Wisconsin Elections Commission:

- *work with the Wisconsin Elections Commission to retract the statutorily noncompliant written guidance for establishing polling places;*

- *promulgate administrative rules to specify the circumstances when municipal clerks can relocate polling places without approval from municipal governing bodies, if the Wisconsin Elections Commission believes municipal clerks should be allowed to relocate polling places in these circumstances; and*

- *report to the Joint Legislative Audit Committee by March 31, 2022, on their efforts to implement these recommendations.*

Issue for Legislative Consideration

The Legislature could consider modifying statutes to allow new polling places to be quickly established in certain situations.

The Legislature could consider modifying statutes to allow new polling places to be quickly established in certain situations, such as in a public health emergency or if a fire or a natural disaster were to damage a polling place to the extent that it could not be used on Election Day. Statutes could specify the situations, if any, in which a municipal clerk could establish polling places without approval from a municipal governing body. For example, a clerk could be given the authority to establish a new polling place for one election if certain types of situations occurred shortly before Election Day. Doing so would help to prevent individuals from being disenfranchised if a polling place were closed shortly before Election Day and insufficient time remained for a municipal governing body to establish a new polling place.

Reconciliation Process

Statutes require municipal clerks to electronically report to WEC certain information no later than 30 days after each primary and each election in which a state or national office is filled.

Statutes require municipal clerks to electronically report to WEC and the relevant county clerk certain information no later than 30 days after each primary and each election in which a state or national office is filled. This information must include the number of individuals who voted, the number who voted by absentee ballot, and the number who registered to vote before or on Election Day. Statutes require WEC to publish and then update this information on its website each month. After polls close on Election Day, poll workers record on the Election Day forms information such as the number of individuals who voted, as determined either by electronic voting equipment or poll workers who hand-counted the ballots. After an election, municipal clerks enter information from these forms into WisVote.

WEC's staff developed a reconciliation process to help municipal clerks accurately report the statutorily required information.

WEC's staff developed a reconciliation process to help municipal clerks accurately report the statutorily required information. WisVote informs clerks if information entered from the Election Day forms is inconsistent with other information in WisVote, such as the number of individuals who voted, and instructs them to determine the reasons for the inconsistencies. If inconsistencies cannot be reconciled, clerks enter into WisVote comments that WEC's staff subsequently review.

As of September 2021, clerks of:

- 1,679 municipalities (90.8 percent) had entered into WisVote consistent information about the number of individuals who had voted in the November 2020 General Election;

- 164 municipalities (8.9 percent) had not entered into WisVote consistent information pertaining to 0.1 percent of all ballots cast in the General Election; and

- 6 municipalities (0.3 percent) had not entered any of this information into WisVote.

Clerks for 106 of the 164 municipalities entered information indicating that a total of 2,840 more individuals had voted than the number of ballots cast. We reviewed comments that WEC's staff had received from clerks in the three municipalities where the number of individuals who voted exceeded by the largest amounts the number of ballots cast, and we asked WEC's staff to provide us with additional information. These comments and information indicated that:

- poll workers in one municipality did not use a sequential number of voting slips on Election Day, which made the number of individuals who voted erroneously appear to be larger than the number of ballots cast;

- poll workers in a second municipality did not enter information from the Election Day forms into WisVote about the number of absentee ballots cast, although the poll books indicated that the individuals who cast these absentee ballots had voted; and

- poll workers in a third municipality did not count 386 absentee ballots on Election Day, although the poll books indicated that the individuals who cast these absentee ballots had voted. These 386 absentee ballots were counted during the subsequent recount.

Clerks for 58 of the 164 municipalities entered information indicating that a total of 186 more ballots were cast than the number of individuals who signed the poll books. We reviewed comments that WEC's staff had received from clerks in the four municipalities where the number of ballots cast exceeded by the largest amounts the number of individuals who voted. These comments indicated that:

- One municipality reported that 41 more ballots were cast than the number of individuals who

signed the poll books. After paper jams occurred while electronic voting equipment was counting ballots, poll workers remade ballots that they were uncertain the equipment had counted.

- A second municipality reported that 19 more ballots were cast than the number of individuals who signed the poll books. This occurred, in part, as a result of paper jams. Poll workers erroneously believed that the electronic voting equipment had not counted the ballots before the jams occurred and thus had the equipment count the ballots a second time.

- Two municipalities each reported that 12 more ballots were cast than the number of individuals who signed the poll books. The two clerks indicated that electronic voting equipment issues caused the differences in the number of ballots cast and the number of individuals who signed the poll books. For example, paper jams resulted in one or more ballots being counted twice because poll workers erroneously believed that the equipment had not counted the ballots before the jams occurred and thus had the equipment count the ballots a second time.

The inconsistent information that municipal clerks entered into WisVote represented 0.1 percent of all ballots cast in the November 2020 General Election. Although some of the inconsistencies resulted from administrative errors, such as not entering information in WisVote, other inconsistencies resulted from ballots having not been properly counted on Election Day. Using the knowledge gained from the General Election, WEC's staff should take additional actions to address such circumstances and improve ballot processing in future elections. For example, WEC's staff could provide additional training to clerks.

☑ Recommendation

We recommend staff of the Wisconsin Elections Commission:

- *take additional actions to improve ballot processing in future elections, such as by providing additional training to clerks; and*

- *report to the Joint Legislative Audit Committee by March 31, 2022, on their efforts to implement this recommendation.*

■ ■ ■ ■

Equipment Approval
Equipment Integrity
Satisfaction Levels of Clerks
Administrative Rule Promulgation

Electronic Voting Equipment

Statutes require WEC to approve the types of electronic voting equipment that municipalities are allowed to use, and statutes require municipal clerks to test the equipment.

Statutes require WEC to approve the types of electronic voting equipment municipalities are allowed to use, and statutes require municipal clerks to test each piece of equipment that will count ballots on Election Day. Municipalities with 7,500 or more residents must use electronic voting equipment, and all municipalities must equip each polling place with accessible voting equipment that permits individuals with disabilities to vote without assistance and with the same degree of privacy afforded to individuals without disabilities. All electronic voting equipment must generate a paper record of all votes cast. We contacted 47 clerks, reviewed 175 statutorily required tests that municipal clerks conducted on the equipment before the November 2020 General Election, and in July 2021 observed the results of the Special Election for the 37th Assembly District being electronically transmitted from polling places to the Dane County clerk's office. We recommend WEC's staff provide additional training to clerks on completing the pre-election tests, reviewing Election Day forms after each election, and investigating relevant issues. We also recommend WEC's staff work with WEC to promulgate statutorily required administrative rules to help ensure the security of software components in equipment. We also include two issues for legislative consideration.

Equipment Approval

Before WEC approves a given type of electronic voting equipment for use in Wisconsin, administrative rules require an equipment's vendor to submit certain documentation, including technical manuals, a list of the states and municipalities where the equipment is approved for use, and reports from an independent testing authority that demonstrate the equipment conforms to Federal Election Commission standards.

Administrative rules require WEC's staff to conduct three mock elections to ensure the equipment meets statutory requirements, including:

- generating a paper record of all votes cast;
- enabling individuals to vote in secrecy, for candidates from different parties, and for write-in candidates;
- allowing individuals to verify their votes, and change their votes or obtain replacement ballots;
- preventing individuals from voting in the primaries of multiple political parties, for more candidates than a contest permits, or multiple times for the same candidate;
- recording correctly and counting accurately every vote properly cast and maintaining a cumulative tally of votes that is retrievable if a power outage or malfunction occurs; and
- minimizing the possibility of disenfranchising individuals as a result of their inability to understand how the equipment operates.

Our review of the documentation submitted by the vendor of one type of equipment found that it included all information required by administrative rules. WEC's staff reviewed the documentation, tested the equipment, and recommended that WEC approve the equipment. In December 2019, WEC approved the equipment for use in Wisconsin.

Administrative rules allow WEC to convene an advisory panel of local election officials and electors to help it review electronic voting equipment being considered for approval. In April 2021, we observed a meeting of this panel, which reviewed two types of equipment being considered for approval for use in the state. During this meeting, the vendor demonstrated the equipment and responded to questions from panel members, who included municipal clerks. WEC's staff indicated that they used input from panel members, as well as the results of the three required mock elections that they later conducted, when WEC's staff subsequently recommended approval of both types of equipment. In June 2021, WEC approved both types of equipment for use in Wisconsin.

Types of Equipment Used

In November 2020, municipalities used seven types of electronic voting equipment that require individuals to mark their choices on paper ballots and then automatically tabulate these ballots. Municipalities

also used six types of accessible voting equipment in November 2020, including one type of direct recording equipment that presents individuals with electronic versions of the ballots, presents individuals with paper copies of their completed ballots, and counts their votes electronically. Municipalities that used this type of direct recording equipment hand-counted paper ballots that were not cast on the equipment.

In November 2020, 1,178 municipalities (63.7 percent) used automatic tabulating equipment, and 49 municipalities (2.7 percent) hand-counted all ballots.

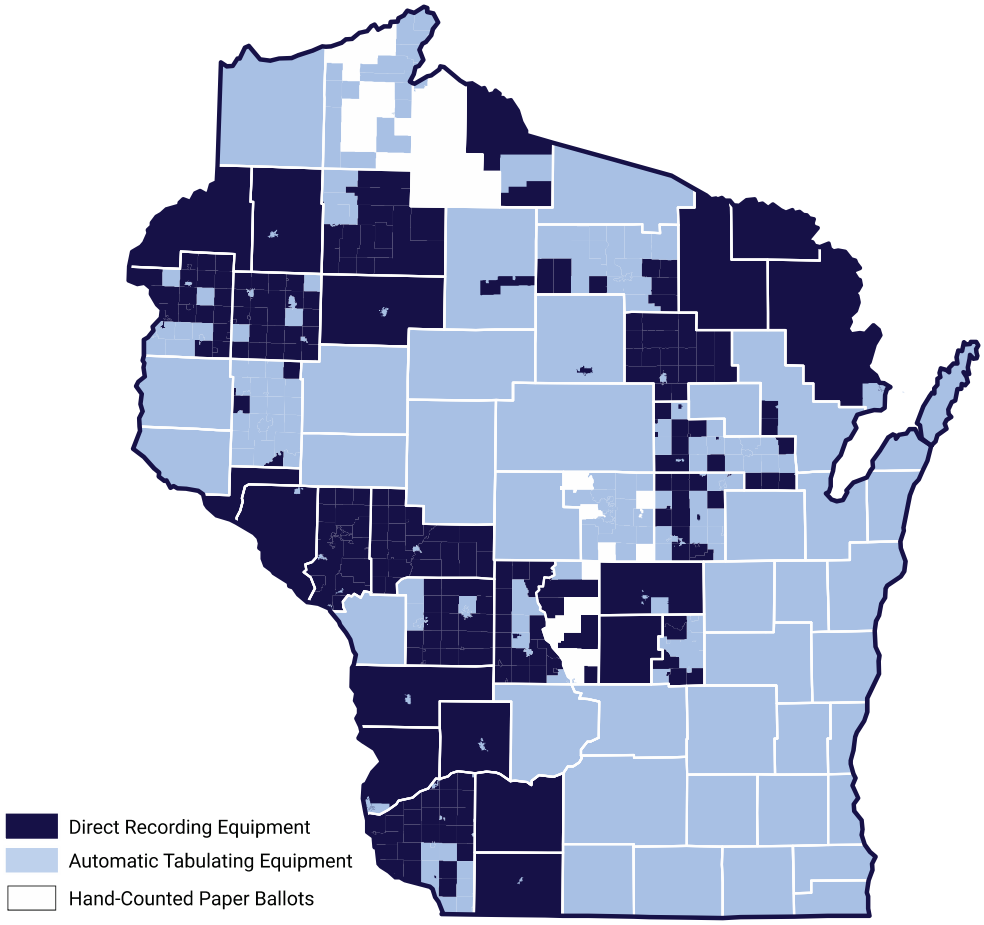
Figure 10 shows the extent to which 1,849 municipalities used electronic voting equipment or hand-counted paper ballots in November 2020. A total of 1,178 municipalities (63.7 percent) used automatic tabulating equipment, 622 municipalities (33.6 percent) used direct recording equipment to electronically count some ballots and hand-counted other ballots, and 49 municipalities (2.7 percent) hand-counted all ballots. In recent years, more municipalities began using electronic voting equipment. In report 14-14, we found that 921 municipalities (49.7 percent) used a type of automatic tabulating equipment, 899 municipalities (48.5 percent) hand-counted all ballots, and 32 municipalities (1.7 percent) used direct recording equipment in January 2014.

Administrative rules require vendors to inform WEC of any modifications they make to previously approved electronic voting equipment. WEC may require the equipment to be reapproved if the modifications are significant. Vendors may not offer for use, sale, or lease any modified equipment in Wisconsin if WEC notifies the vendors that the equipment must be reapproved. We reviewed materials for all meetings that WEC held from January 2020 through June 2021 and found that WEC's administrator approved 12 modifications, as permitted under the authority WEC delegated to the administrator, and informed WEC about these approvals. The materials indicated that WEC's staff had obtained and assessed information from the vendors before the administrator approved the modifications.

Statutes allow WEC to revoke its approval of a given type of electronic voting equipment at any time for cause. In September 2017, WEC approved a timeline to revoke its approval of one type of equipment, which WEC determined could no longer be used in Wisconsin beginning in January 2019 because of concerns that the equipment might not count ballots marked with writing utensils other than pencils and vendor-approved markers. WEC approved specific ballot-counting procedures that municipalities were required to implement if they continued to use the equipment before January 2019. We found that WEC's staff communicated these procedures to municipalities in a timely manner.

Figure 10

Use of Electronic Voting Equipment and Hand-Counted Paper Ballots[1]
November 2020



[1] According to information reported by municipalities to WEC. Municipalities that used direct recording equipment also hand-counted ballots.

Issue for Legislative Consideration

The Legislature could consider modifying statutes to require municipal clerks to notify WEC's administrator if they rent electronic voting equipment.

Statutes require municipal clerks to notify WEC's administrator if they adopt and purchase a new or different type of electronic voting equipment. When municipalities rent equipment, such as to count absentee ballots at central count locations during elections at which many individuals are expected to vote, statutes do not require clerks to notify WEC's administrator. The Legislature could consider modifying statutes to require clerks to notify WEC's administrator if they rent electronic voting equipment. Doing so would allow WEC's administrator, and therefore WEC, to know that all equipment used in the state has been approved by WEC.

Equipment Integrity

Statutes include provisions for helping to ensure the integrity of electronic voting equipment, including by requiring that:

- municipal clerks conduct pre-election tests of each piece of equipment that will be used to count ballots in an election; and
- poll workers ensure on Election Day that all equipment used to count ballots has a tamper-evident seal that is intact.

Pre-Election Tests

No more than 10 days before an election, statutes require a municipal clerk to publicly test each piece of electronic voting equipment that will count ballots on Election Day.

No more than 10 days before an election, statutes require a municipal clerk to publicly test each piece of electronic voting equipment that will count ballots on Election Day. Doing so helps to ensure that the equipment counts ballots accurately. During a test, a clerk must process a group of ballots marked to record a predetermined number of votes for each candidate. To determine whether the equipment properly rejects votes, a test must include more votes than allowed for each contest on the ballot, which is termed an over-vote. If the equipment errs in counting the votes, a clerk must determine the cause and correct the error. Statutes require each piece of equipment to make an errorless count before it can be used in an election.

We determined whether a sample of municipal clerks completed the statutorily required tests of electronic voting equipment before the November 2020 General Election and whether a sample of the tests indicated that the equipment counted the predetermined votes accurately. To do so, we requested the results of all pre-election tests that clerks in 29 municipalities throughout Wisconsin conducted and the ballots used in these tests. Appendix 6 summarizes the results of our analysis for each of the 29 municipalities, which included:

- 9 of the 10 municipalities where the most absentee ballots were cast, other than the City of Madison, which did not allow us to physically handle election-related materials;
- the 10 municipalities where absentee ballots made up the largest proportions of the total ballots cast; and
- 10 municipalities we chose at random from counties other than those in which the other 19 municipalities were located.

Statutes allow election-related materials to be destroyed after specified periods of time have elapsed after an election. For example, ballots, applications for absentee ballots, registration forms, or other records and papers requisite to voting in any federal election, other than registration cards, can be destroyed after 22 months. If statutes do not specify how long a particular type of election-related material must be retained, statutes indicate that the material may be destroyed after 90 days. WEC's staff indicated that statutes do not specify how long the pre-election test results must be retained, and clerks did not agree on how long they must be retained. Some clerks indicated that the results must be retained for 22 months, while other clerks indicated that the results must be retained for 90 days.

Clerks provided us with the results of all statutorily required pre-election tests in 16 of 29 municipalities.

Clerks provided us with all statutorily required pre-election test results in 16 of 29 municipalities, some test results in 9 municipalities, and no test results in 4 municipalities. Clerks in the nine municipalities provided us with either no results of some tests or incomplete documentation of tests that were conducted. Some of these clerks were unable to find complete test results or no longer retained the test results.

Municipal clerks conducted 88 of 175 pre-election tests (50.3 percent) within the statutorily prescribed 10 days before theNovember 2020 General Election.

Among the 175 pre-election test results that we examined, we found that municipal clerks:

- conducted 88 tests (50.3 percent) within the statutorily prescribed 10 days before the November 2020 General Election; and
- conducted 87 tests (49.7 percent) more than 10 days before the General Election. These 87 tests were conducted between 11 and 22 days before the General Election.

In total, 59 of the 60 pre-election test results we examined indicated that the electronic voting equipment had accurately counted the votes for presidential candidates.

We reviewed in greater detail 60 of the 175 pre-election test results and determined whether the electronic voting equipment had accurately counted the votes for presidential candidates. To do so, we hand-counted the number of votes for each candidate, as indicated on the predetermined paper ballots used in the tests, and compared the results to the number of votes the equipment had counted during the tests. We found that:

- 59 of the 60 test results indicated that the equipment had accurately counted the votes for presidential candidates; and
- 1 test result included insufficient documentation, which prevented us from determining whether the equipment had accurately counted the votes for presidential candidates.

Our review of the 60 pre-election test results also found that three pre-election tests conducted in three municipalities excluded the statutorily required over-votes on the predetermined ballots. One clerk indicated unfamiliarity with testing over-votes on newly purchased electronic voting equipment, a second clerk indicated that the test mistakenly excluded the over-votes, and a third clerk indicated that over-votes were never included in the tests.

WEC's staff should provide additional training to municipal clerks on completing the statutorily required pre-election tests of electronic voting equipment. Such training should emphasize the statutory requirement for clerks to complete the pre-election tests within 10 days before an election and for the tests to include over-votes on the predetermined ballots.

☑ Recommendation

We recommend staff of the Wisconsin Elections Commission:

- *provide additional training to municipal clerks on completing the statutorily required pre-election tests of electronic voting equipment; and*
- *report to the Joint Legislative Audit Committee by March 31, 2022, on their efforts to implement this recommendation.*

Tamper-Evident Seals

Statutes require each piece of electronic voting equipment that will count ballots to have a tamper-evident seal.

Statutes require each piece of electronic voting equipment that will count ballots to have a tamper-evident seal. These seals are affixed after clerks have conducted the pre-election tests in order to secure the equipment in preparation for an upcoming election. On Election Day, statutes require poll workers to sign an Election Day form indicating that they verify having examined the seals and that they certify the integrity of the seals. These forms include spaces for chief election inspectors to write their initials and thereby certify the integrity of the seals when the polls opened and when the polls closed.

We selected a random sample of 319 municipalities and requested that the relevant county clerks provide us with all of the Election Day forms that poll workers in these municipalities completed on Election Day in November 2020 at polling locations other than central count locations. These municipalities, which are located in 69 counties, are listed in Appendix 5. We received forms for all 319 municipalities.

A total of 513 of 589 Election Day forms (87.1 percent) contained the expected initials of poll workers, who thereby certified the integrity of the tamper-evident seals.

Among the 589 Election Day forms we included in this analysis:

- 513 forms (87.1 percent) contained the expected initials of poll workers, who thereby certified the integrity of the tamper-evident seals when the polls opened and when they closed; and

- 76 forms (12.9 percent) did not contain all of the expected initials of poll workers, including 42 forms without initials certifying seal integrity when the polls opened and when they closed, 31 forms without initials certifying seal integrity when the polls closed, and 3 forms without initials certifying seal integrity when the polls opened. The forms without initials may indicate poll workers found problems with the seals or forgot to initial the forms.

WEC's staff indicated that some poll workers may be hesitant to certify the integrity of the tamper-evident seals, in part, because of unfamiliarity with the electronic voting equipment and uncertainty about how to ascertain seal integrity. However, WEC's staff indicated that certifying seal integrity helps to instill confidence in the public that the equipment has not been tampered with before an election. WEC's staff should provide training to municipal clerks on reviewing the Election Day forms after each election and investigating relevant issues, such as forms on which poll workers have not certified the integrity of the tamper-evident seals on electronic voting equipment. By investigating such issues, a clerk could ascertain whether poll workers forgot to initial the forms or the seals were not intact and, as a result, a given clerk needs to investigate the ramifications of seals that were not intact. Investigating such issues may reveal the need for clerks to provide additional training to poll workers.

☑ Recommendation

We recommend staff of the Wisconsin Elections Commission:

- *provide training to municipal clerks on reviewing Election Day forms after each election and investigating relevant issues, including those related to tamper-evident seals; and*

- *report to the Joint Legislative Audit Committee by March 31, 2022, on their efforts to implement this recommendation.*

Issue for Legislative Consideration

The Legislature could consider modifying statutes to explicitly require materials related to the pre-election tests of electronic voting equipment to be retained for 22 months.

The Legislature could consider modifying statutes to explicitly require materials related to the pre-election tests of electronic voting equipment to be retained for 22 months after a federal election. Doing so would ensure that these pre-election test materials, which indicate whether electronic voting equipment counted ballots accurately, are retained for the same period of time as other election-related materials such as ballots and applications for absentee ballots.

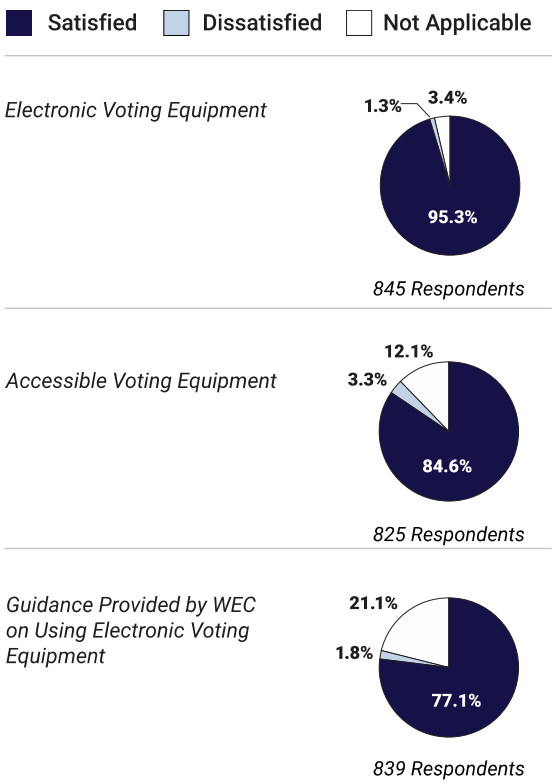
Satisfaction Levels of Clerks

Most municipal clerks who responded to our survey were satisfied with the electronic voting equipment.

Our April 2021 survey asked municipal clerks about their electronic voting equipment. As shown in Figure 11, most municipal clerks who responded to our survey were satisfied with the electronic voting equipment, the accessible voting equipment, and guidance from WEC on using this equipment.

Figure 11

Satisfaction of Municipal Clerks with the Electronic Voting Equipment Used in the November 2020 General Election[1]

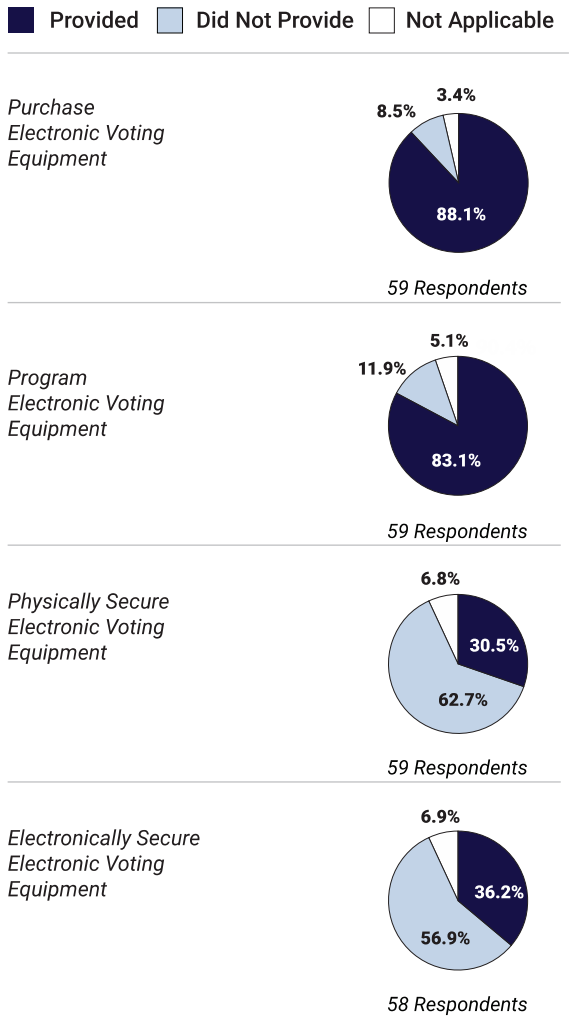


[1] As indicated by municipal clerks who responded to our April 2021 survey.

Our survey asked county clerks about the assistance they provided to municipalities. As shown in Figure 12, most county clerks who responded to our survey indicated that they helped municipalities to purchase and program electronic voting equipment. Approximately one-third of county clerks indicated that they helped municipalities to physically or electronically secure the equipment.

Figure 12

Types of Assistance that County Clerks Provided to Municipalities[1]



[1] As indicated by county clerks who responded to our April 2021 survey.

We contacted 40 municipal and 7 county clerks to obtain additional information. Similar to our survey results, these clerks indicated general satisfaction with the electronic voting equipment. For example:

- one clerk indicated that the equipment accurately counted ballots;
- a second clerk indicated that the security and reliability of the equipment was fantastic; and
- a third clerk indicated that WEC's staff frequently provided updated information, webinars, and other materials that enabled the clerk to handle all types of issues on Election Day.

We contacted clerks who had indicated in their survey responses dissatisfaction with the electronic voting equipment. For example:

- one clerk indicated that accessible voting equipment is expensive, requires significant storage space between elections, and is rarely used on Election Day;
- a second clerk indicated that the equipment is complicated, difficult to understand, and expensive; and
- a third clerk indicated that a printing error prevented absentee ballots from being fed into the equipment correctly and, as a result, a poll worker needed to remake ballots.

Administrative Rule Promulgation

WEC did not comply with statutes by promulgating administrative rules to address security-related issues for electronic voting equipment.

Statutes require WEC to promulgate administrative rules that ensure the security, review, and verification of the software components used with electronic voting equipment approved by WEC. Administrative rules contained requirements for vendors to submit certain documents that allow WEC's staff to review and verify such equipment, including the software components. However, we found that the administrative rules did not address security-related issues.

WEC's staff should work with WEC to promulgate the statutorily required administrative rules. These administrative rules should include provisions that help to ensure the security of the software components in electronic voting equipment approved by WEC.

☑ Recommendation

We recommend staff of the Wisconsin Elections Commission:

- *work with the Wisconsin Elections Commission to promulgate statutorily required administrative rules for helping to ensure the security of software components in approved electronic voting equipment; and*

- *report to the Joint Legislative Audit Committee by March 31, 2022, on their efforts to implement this recommendation.*

■ ■ ■ ■

Post-Election Audit

After each General Election, statutes require WEC to audit the performance of each type of electronic voting equipment.

After each General Election, statutes require WEC to audit the performance of each type of electronic voting equipment and determine the equipment's error rate in counting ballots. If the error rate exceeds the standards of the Federal Election Commission that were in effect on October 29, 2002, statutes require WEC to take remedial action and order affected counties and municipalities to take remedial action to ensure compliance with the standard. We reviewed the results of the audit completed after the November 2020 General Election. We recommend WEC's staff provide municipal clerks with additional training and guidance on ensuring that ballots are counted accurately when paper jams occur in equipment, as well as comply with statutes by calculating an error rate for each type of equipment. We also include two issues for legislative consideration.

Post-Election Audit Procedures

Statutes do not stipulate how the post-election audits are to be conducted. In September 2020, WEC established that the audit for electronic voting equipment to be used in the November 2020 General Election should include:

- each piece of equipment used in a sample of 5.0 percent of the state's 3,698 reporting units, which are either a single ward or multiple wards that report combined election results;

- at least one piece of equipment used in each county;

- at least five reporting units that used each type of equipment certified for use in the state; and

- the equipment used in up to four reporting units in the cities of Milwaukee and Madison, up to three reporting units in the 20 other largest municipalities, and up to one reporting unit in all other municipalities.

WEC's staff selected 190 reporting units to include in the post-election audit, but these included 7 reporting units in which no individuals voted in November 2020. As a result, the audit included 183 reporting units in 163 municipalities, and we found that it complied with the selection procedures that WEC had approved in September 2020.

Municipal clerks and local election officials completed the post-election audit work based on procedures provided by WEC's staff.

Municipal clerks and local election officials completed the post-election audit work based on procedures provided by WEC's staff. The procedures specified that at least two individuals should hand-count each ballot based on how the electronic voting equipment would have counted it, without considering voter intent. For example, if a voter had circled the name of a candidate on a ballot but had not filled in the oval next to the candidate's name, the equipment likely would not have considered that to be a vote for the candidate. The procedures instructed auditors to compare their hand-counted results to the results provided by the equipment on Election Day and provide reasonable explanations for any discrepancies in the results. We contacted 10 municipal clerks who were involved in the post-election audit. These clerks indicated that they were generally satisfied with the audit procedures and training that WEC's staff had provided them.

Statutes do not specify the date by which the audit must be completed. In report 14-14, we found that local election officials had conducted the electronic voting equipment audits associated with the November 2008, November 2010, and November 2012 General Elections and informed GAB that they had done so. However, not until October 2013 did GAB's staff complete the statutorily required post-election audits of the equipment that had been used in these three elections. In our current audit, we found that WEC established a deadline for completing the post-election audit before December 1, 2020, which was the statutory deadline for certifying the election results. All municipalities conducted their audits by that date.

WEC voted to reimburse municipalities $50 per reporting unit, plus $0.35 per audited ballot. According to information that WEC's staff provided to WEC in February 2021, 154 municipalities had requested reimbursement totaling $55,400.

Post-Election Audit Results

According to WEC's Election Day manual, electronic voting equipment indicates when an individual votes for more candidates than allowed in a given contest, which is termed an over-vote. When this occurs, the manual instructs poll workers to offer individuals who vote in person at

polling places the opportunity to spoil their ballots and record their votes on new ballots. The manual instructs poll workers to review absentee ballots containing over-votes and, if voter intent can be determined, remake absentee ballots so that the equipment will count the votes.

WEC's staff determined that the electronic voting equipment for the most part accurately counted ballots, but they identified an issue with one type of equipment.

WEC's staff compiled the audit results provided by municipal clerks into a February 2021 report to WEC. This report indicated that 145,100 ballots were hand-counted during the audit, which determined that the electronic voting equipment for the most part accurately counted ballots in the November 2020 General Election. However, the report identified an issue with the equipment in 2 of the 28 reporting units that were audited and used this equipment. When absentee ballots were folded for mailing and creases ran through the write-in fields for certain contests, the equipment considered the creases to be votes because it was programmed to read marks in the write-in fields. If an individual actually voted for a candidate in one of these contests, the equipment concluded that the individual had voted both for that candidate and a write-in candidate. When an individual casts a ballot containing an over-vote, the equipment does not count any vote for that contest. WEC's staff reported that administrative procedures, rather than malfunctioning equipment, caused this issue, which affected 26 of the 2,747 ballots cast in these two reporting units.

In February 2021, WEC directed its staff to obtain reports from county clerks on the number of over-votes counted by the particular type of electronic voting equipment statewide. In March 2021, WEC's staff reported to WEC that municipalities in 19 counties had used this equipment in the November 2020 General Election, including municipalities in 12 counties that had used equipment programmed to read only marks in the ovals next to the names of write-in candidates. WEC's staff determined that the equipment did not count as over-votes the creases in ballots cast in these 12 counties. In contrast, municipalities in seven counties had used equipment programmed to read marks both in the ovals and the write-in fields and, as a result, the equipment counted as over-votes the creases in ballots cast in these seven counties.

WEC's staff examined 1,109 ballots cast in the seven counties and determined that:

- 724 over-votes occurred because of creases through the write-in fields;
- 376 over-votes occurred because of marks made by individuals who had, for example, voted for multiple candidates in a given contest or attempted to correct errors that they had made on ballots; and
- 72 over-votes occurred for other inadvertent reasons, such as ink that bled through ballots because individuals had voted for candidates on both sides of a given ballot.

Table 7 shows the seven counties and the contests in which the 724 over-votes occurred because of ballot creases. WEC's staff

determined that the over-votes did not change the outcome of any contest. A total of 336 of the 724 over-votes (46.4 percent) occurred in uncontested contests. If the over-votes had not occurred on the ballots for the state senator contest in Winnebago County, 202 votes would have been counted for the losing candidate and 129 votes would have been counted for the winning candidate, who won by more than 16,000 votes.

Table 7

Over-Votes Caused by Ballot Creases, by County and Contest[1]
November 2020 General Election

County	President	State Senator	Assembly Representative	County Treasurer[2]	County Register of Deeds[2]	Total
Door	1					1
Green					87	87
Ozaukee		2		163		165
Vilas		1	5		37	43
Walworth	1		16		1	18
Washington	1	11		7	42	61
Winnebago	1	331	17			349
Total	**4**	**345**	**38**	**170**	**167**	**724**

[1] As determined by WEC's staff.

[2] All contests except for the Walworth County Register of Deeds were uncontested.

We reviewed 1,109 over-voted ballots cast in seven counties and found 468 over-votes occurred for reasons other than ballot creases.

We reviewed electronic copies of all 1,109 ballots from the seven counties that contained over-votes. We found that 468 over-votes occurred for reasons other than ballot creases, including 391 over-votes that occurred because of marks on the ballots made by individuals, 42 over-votes that occurred because ink bled through ballots, and 35 over-votes that occurred because a vertical line printed on ballots made marks in write-in fields. The electronic voting equipment did not count how the individuals voted in the contests involving the 468 over-votes.

In March 2021, WEC's staff indicated to WEC that they planned to emphasize in future training sessions for municipal clerks the importance of reviewing over-votes. We found that WEC's staff subsequently provided municipal clerks with additional training materials, including a webinar. We reviewed these materials and the webinar and found that they included information on ballots with over-votes and provided detailed instructions on how to remake them. We reviewed the post-election audit results reported by municipal clerks to WEC's staff and found no differences between the Election

Day results and the audit results in 110 of the 183 reporting units (60.1 percent), but we found differences in 73 reporting units (39.9 percent). Most of these differences involved one vote or one ballot. One difference involved 21 ballots, which was the largest difference and which occurred because of ballot creases through the write-in fields. The most-common reason for a difference was a paper jam when ballots were fed into the equipment or the paper roll on which ballots were printed was replaced in the equipment, which occurred in 22 reporting units.

WEC's staff should ensure equipment vendors provide municipal clerks with additional training on ensuring that ballots are counted accurately when paper jams occur in electronic voting equipment.

Paper jams do not always result in electronic voting equipment inaccurately counting ballots. However, when paper jams occur, poll workers need to know how to ensure that ballots are counted accurately. Given the results of the post-election audit, WEC's staff should ensure equipment vendors provide municipal clerks with additional training on ensuring that ballots are counted accurately when paper jams occur in equipment.

☑ Recommendation

We recommend staff of the Wisconsin Elections Commission:

- *ensure equipment vendors provide additional training to municipal clerks on ensuring that ballots are counted accurately when paper jams occur in electronic voting equipment; and*

- *report to the Joint Legislative Audit Committee by March 31, 2022, on their efforts to implement this recommendation.*

Equipment Error Rate

As noted, statutes require WEC to determine an error rate for each type of electronic voting equipment after each General Election. The Federal Election Commission's standards that were in effect on October 29, 2002, specified that equipment should have an error rate that does not exceed one vote per 500,000 ballot positions, which is every choice that an individual could make when marking a ballot, including for write-in candidates. For example, if a ballot allowed an individual to vote for three candidates or write in a candidate, that ballot would have four ballot positions. If a given type of equipment exceeds the error rate, statutes require WEC to take remedial action and order affected counties and municipalities to take remedial action to ensure compliance with the standard. WEC's staff indicated that such remedial action may include amending the certification of the equipment, decertifying the equipment, or providing updated guidance to clerks on using the equipment.

WEC's staff did not report to WEC the statutorily required error rates for any types of electronic voting equipment used in the November 2020 General Election.

WEC's staff did not report to WEC the statutorily required error rates for any types of electronic voting equipment used in the November 2020 General Election. The report WEC's staff provided to WEC in February 2021 indicated that the error rate is intended for equipment certification testing conducted in laboratory settings under optimized conditions, including by using ballots marked according to instructions, rather than typical absentee ballots that contain imperfections. The report also indicated that post-election audits require municipal clerks to use their best judgement when determining how the equipment counted ballots with ambiguous marks.

WEC's staff recommended that WEC amend the certification for the electronic voting equipment that had considered ballot creases through write-in fields to be votes. In February 2021, WEC approved this recommendation to require that the equipment be programmed to ensure that creases or marks in the write-in fields are not counted as votes. We found that WEC's staff sufficiently informed county and municipal clerks about the amended certification. Nevertheless, WEC's staff should comply with statutes by calculating an error rate for each type of equipment after each General Election.

☑ Recommendation

We recommend staff of the Wisconsin Elections Commission:

- *comply with statutes by calculating an error rate for each type of electronic voting equipment used in each General Election; and*
- *report to the Joint Legislative Audit Committee by March 31, 2022, on their efforts to implement this recommendation.*

Post-Election Audits in Other States

In Wisconsin, a post-election audit determines whether the electronic voting equipment counted ballots according to how it was programmed to count them. However, such an audit does not determine the validity of election results because it does not consider voter intent, and it does not necessarily review a sufficiently large sample of ballots needed to determine the validity of election results.

A risk-limiting audit uses statistical methods to review a sample of ballots cast in order to determine voter intent and the validity of the election results.

Figure 13 summarizes key characteristics of three types of post-election audits, including the traditional type used in Wisconsin and a procedural audit. A risk-limiting audit uses statistical methods to review a sample of ballots cast in order to determine voter intent and the validity of the election results. The number of ballots reviewed in a risk-limiting audit depends on the election results. If a given candidate's margin of victory is small, more ballots must be reviewed. If the initial results of the audit do not confirm the election results, additional ballots must be reviewed until the audit confirms the election results. If the additional ballots do not

confirm the election results, a full recount may need to be conducted in order to determine the results.

Figure 13

Types of Post-Election Audits[1]

TRADITIONAL	PROCEDURAL	RISK-LIMITING
Examines a fixed proportion of reporting units or electronic voting equipment and compares paper ballot results to equipment-generated results; and audits the same number of ballots regardless of election results	Ensures prescribed processes and procedures were followed during an election	Uses statistical methods to review a sample of ballots cast in order to determine voter intent and the validity of the election results; reviews more ballots when a candidate's margin of victory is small

[1] According to information from NCSL.

Information from NCSL in February 2020 indicated that at least six states—Colorado, Georgia, Indiana, Nevada, Rhode Island, and Virginia—conducted risk-limiting audits or planned to conduct them, and four states—California, Ohio, Oregon, and Washington—provided options for different types of audits, including risk-limiting audits, that can be conducted. Counties typically conducted these audits.

The cost of risk-limiting audits varies. Such an audit may be less expensive when the winning candidate has a large margin of victory, but it may be more expensive in tighter contests or when the initial audit results do not match the election results and the audit must be expanded to review more ballots or to conduct a full recount.

Issues for Legislative Consideration

The Legislature could consider modifying statutes to reflect the current federal standards for an acceptable equipment error rate.

As noted, statutes require WEC to take remedial action if the error rate found in electronic voting equipment exceeds the federal standards that were in effect on October 29, 2002, which was one vote per 500,000 ballot positions. We found that these standards were updated in 2015 to specify that the maximum acceptable error rate is 1 vote per 125,000 contests counted by a given type of equipment. Calculating the error rate based on the number of contests, rather than the number of ballot positions, is more straightforward because ballot positions may vary within and among municipalities, depending on the number of

candidates in each contest. The Legislature could consider modifying statutes to reflect the current federal standards for an acceptable equipment error rate.

The Legislature could consider modifying statutes to require WEC to conduct risk-limiting post-election audits.

The Legislature could consider modifying statutes to require WEC to conduct risk-limiting post-election audits. Such audits are intended to determine voter intent and determine the validity of the election results, which may be preferable to the current audits that confirm whether the equipment counted ballots according to how it was programmed. As noted, one type of equipment was programmed in such a way that it counted ballot creases as votes in some counties during the November 2020 General Election.

■ ■ ■ ■

Complaints Filed with Clerks

Our April 2021 survey asked all municipal and county clerks about the written complaints they had received concerning the November 2020 General Election.

Our April 2021 survey asked all municipal and county clerks about the written complaints they had received concerning the November 2020 General Election. We defined a complaint to include issues identified in writing by individuals, including those who identified themselves and those who were anonymous. A total of 59 county clerks (81.9 percent of the total) and 848 municipal clerks (46.2 percent) responded to our survey questions about election-related complaints. Most respondents indicated that they had received no written complaints about the General Election. We contacted 43 clerks, including 33 municipal clerks and 10 county clerks, in order to obtain additional information about complaints they had received and actions they had taken in response to the complaints.

Number of Complaints

In response to our survey, most clerks indicated that they had received no written complaints about the November 2020 General Election.

Our survey asked clerks to indicate a range that described the number of written complaints they had received about the November 2020 General Election. Of the 848 municipal clerks and 59 county clerks who responded to our survey:

- 791 municipal clerks (93.3 percent) and 38 county clerks (64.4 percent) indicated that they had received no written complaints; and

- 57 municipal clerks (6.7 percent) and 21 county clerks (35.6 percent) indicated that they had each received from 1 to 25 written complaints. Appendix 12 lists the locations of these clerks.

Our survey asked the 57 municipal clerks and the 21 county clerks to indicate the issues discussed in the written complaints they had received about the November 2020 General Election. As shown in Table 8, 35 clerks indicated that they had received written complaints pertaining to absentee ballots. Clerks could indicate having received written complaints about multiple issues.

Table 8

Written Complaints That Clerks Received about the November 2020 General Election, by Issue[1]
As of April 2021

Issue	Number of Clerks		
	Municipal Clerks	County Clerks	Total
Absentee Ballots	27	8	35
Alleged Voter Fraud	16	7	23
Electronic Voting Systems	9	9	18
Polling Place Practices	10	4	14
Voter Registration	5	0	5
Other[2]	23	7	30

[1] As indicated by 57 municipal clerks and 21 county clerks who responded to our April 2021 survey. Clerks could indicate having received written complaints about multiple issues.

[2] Includes complaints about the MyVote Wisconsin website, polling place locations, potential illegal activity, in-person voting, and possible election misinformation.

We contacted 43 clerks to obtain additional information about complaints they had received. We selected most of these clerks because they had indicated in their survey responses that they had received written complaints about the November 2020 General Election, but we also contacted five clerks who had not responded to our survey.

A total of 25 of the 43 clerks (58.1 percent) we contacted indicated that they had received written complaints about the November 2020 General Election, and 30 of the 43 clerks (69.8 percent) indicated that they had received verbal complaints about the General Election. The number of complaints that a given clerk received was not related to the population of that clerk's municipality or county. Clerks reported having received verbal complaints regarding topics that were similar to those raised in the written complaints that they reported in the survey. Nine clerks indicated that they had received at least one complaint that was based on a media report a complainant had heard or read.

Clerk Actions

In response to our survey, 44 clerks indicated that they had investigated issues pertaining to at least one written complaint.

Our survey asked clerks whether they had taken specific actions after having received written complaints about the November 2020 General Election. As shown in Table 9, 44 clerks indicated that they had investigated issues pertaining to at least one written complaint.

Table 9

Actions Taken by Clerks Who Received Written Complaints about the November 2020 General Election[1]
As of April 2021

Action Taken	Number of Clerks		
	Municipal Clerks	County Clerks	Total
Conducted an investigation	38	6	44
Provided an individual with information about filing a complaint with WEC	11	7	18
Referred a complaint to a district attorney	4	1	5
Other[2]	6	4	10

[1] As indicated by 57 municipal clerks and 21 county clerks who responded to our April 2021 survey. Clerks could indicate having taken multiple actions.

[2] Includes providing information to individuals about election laws and procedures and forwarding complaints to local law enforcement agencies.

Many of the 43 clerks we contacted provided us with specific examples of how they had handled complaints about the November 2020 General Election. For example:

- One municipal clerk reported having received one verbal complaint by a voter who was upset about having been asked at a polling place to remove a hat with a political statement on it. The clerk explained to the voter that wearing political apparel at a polling place, which is a form of electioneering, is prohibited by state law.

- A second municipal clerk reported having received from 10 to 20 written complaints about various misunderstandings about election laws and procedures. The clerk also reported having received from 10 to 20 verbal complaints, most of which pertained to issues about absentee ballots. The clerk

indicated having provided all of these individuals with information to address their complaints.

- A third municipal clerk reported having received one verbal complaint about an individual who allegedly did not live in the municipality but was registered to vote there. The clerk referred the complaint to WEC. The clerk also reported having received one written complaint from an individual who alleged that all registered voters had received absentee ballots. After reviewing information in WisVote, the clerk determined that the individual had received an absentee ballot because the individual had previously registered as being indefinitely confined. At the individual's request, the clerk removed the individual from the list of indefinitely confined individuals.

- A fourth municipal clerk reported having received at least 70 verbal complaints about a variety of issues, including difficulties receiving and returning absentee ballots, the public health implications of in-person voting, and voter records not being updated immediately after an election. The clerk provided the complainants with information about election laws and procedures. The clerk also reported having received one written complaint about individuals who registered to vote using the address of a UPS mailbox. The clerk found that multiple individuals were registered to vote using this address and referred the issue to WEC and the district attorney. Media reports indicate that the district attorney determined these individuals were eligible voters and declined to file charges against them.

- A fifth municipal clerk reported having received from one to three verbal complaints from individuals whose voting records on the MyVote Wisconsin website had not been updated immediately after the election. The clerk explained to the individuals that clerks have 45 days after an election to update voting records.

- A county clerk reported having received one written complaint from a municipal clerk regarding an Illinois resident who had a Wisconsin driver's license and was registered to vote in the county. Using information from the Chicago Board of Election Commissioners, the county clerk determined that the individual had voted in Wisconsin and Illinois, referred the issue to WEC, and believed that the district attorney became involved.

A number of clerks indicated that handling complaints and administering the November 2020 General Election had caused them distress.

A number of clerks indicated that handling complaints and administering the November 2020 General Election had caused them distress. For example:

- A municipal clerk described stress caused by the need to send out four times the number of absentee ballots as had been sent out for prior presidential elections. The clerk indicated that this task had kept the clerk from fulfilling other job duties. The clerk indicated that potentially being required to send absentee ballots to every registered voter would be an impossible task and, therefore, caused the clerk to consider resigning from the position.

- A second municipal clerk indicated that a number of clerks had talked about resigning from their positions because of the disruptive effects of pre-election rule changes and increased rhetoric regarding elections administration. The clerk indicated an intention to not serve in the position during another presidential election.

Number of Complaints
Concerns
Improving Procedures
Issue for Legislative Consideration

Complaints and Concerns Filed with WEC

Individuals can file election-related complaints and concerns with WEC in multiple ways.

Individuals can file election-related complaints and concerns with WEC in multiple ways. Statutes allow WEC to investigate sworn, written complaints alleging violations of election laws, as well as sworn, written complaints submitted by electors alleging that election officials acted contrary to the law in administering elections. In addition, individuals can provide election-related concerns through forms on WEC's website, email messages, and telephone calls. We found that WEC's staff informed WEC about the status of submitted complaints and handled complaints in a timely manner, but that WEC's staff did not have written policies for handling complaints and did not track how they responded to concerns, which are not sworn complaints. We recommend WEC's staff work with WEC to promulgate administrative rules for handling complaints and tracking concerns, and we include an issue for legislative consideration.

Number of Complaints

Statutes allow WEC to investigate an alleged violation of election laws if a reasonable suspicion exists that a violation occurred or is occurring, and it allows WEC to retain a special investigator. Anyone may submit a sworn, written complaint to WEC alleging such a violation. WEC's staff indicated that the $25,000 appropriated annually for investigations from FY 2016-17 through FY 2020-21 was lapsed each year because WEC has never retained a special investigator.

Statutes allow WEC to investigate whether an election official did not comply with legal requirements pertaining to issues such as elections administration, nominations, candidate qualifications, voting qualifications, ballot preparation, and election conduct. Individuals

may submit a sworn, written complaint to WEC alleging such a violation by an election official in whose jurisdiction they vote.

Statutes allow individuals to submit sworn, written complaints that challenge the nomination papers of a candidate for elected office or the eligibility of a candidate to hold an elected office. WEC's staff consider such complaints to be ballot access challenges. For example, an individual may allege that an individual circulating nomination papers did not properly certify them after obtaining signatures, or that some of the obtained signatures are invalid. WEC's staff separately track this type of complaint because administrative rules require ballot access challenges to be filed within three days after the deadline for filing nomination papers, as well as because a challenge can prevent candidates from being placed on a ballot.

As of late-May 2021, WEC had received 45 complaints regarding the November 2020 General Election.

As of late-May 2021, WEC had received 45 complaints regarding the November 2020 General Election, as shown in Table 10. This total included 18 complaints about the conduct of election officials, 16 complaints about alleged violations of election laws, and 11 ballot access challenges. Individuals who submitted 38 of the 45 complaints indicated that their allegations were based on firsthand knowledge of issues described in their complaints.

Table 10

Complaints Filed with WEC Regarding the November 2020 General Election[1]
As of late-May 2021

Type of Complaint	Number	Percentage of Total
Conduct of Election Officials	18	40.0%
Alleged Violations of Election Laws	16	35.6
Subtotal	34	75.6
Ballot Access Challenges	11	24.4
Total	**45**	**100.0%**

[1] According to information provided by WEC's staff.

Complaint Resolution

Statutes allow WEC to resolve complaints alleging violations of election laws by taking various actions, including assessing a financial penalty up to $2,500 or referring an issue to a district attorney. Statutes allow WEC to resolve complaints about the conduct of election officials by ordering officials to comply with legal requirements, refrain from taking

actions contrary to legal requirements, or correct an action or decision inconsistent with legal requirements. In February 2020, WEC authorized its administrator, in consultation with its chairperson, to resolve complaints about the conduct of election officials.

WEC's staff did not have written policies for considering complaints.

We found that WEC's staff did not have written policies for considering complaints. WEC's staff indicated that they relied on provisions in statutes and administrative rules to guide how they considered complaints. We note that administrative rules promulgated in 1994 describe procedures for considering complaints about the conduct of election officials. However, these administrative rules are no longer in effect for complaints alleging violations of election laws because statutes were modified by 2007 Wisconsin Act 1, which created GAB.

We found that WEC's staff did not request additional information from the individuals who had submitted 42 of the 45 complaints we examined, but they requested additional information from the individuals who had submitted 3 complaints. WEC's staff indicated that they try to minimize the number of times they request additional information from complainants and respondents in order to maintain their impartiality and avoid influencing a complaint's outcome. WEC's staff indicated that they represent WEC in legal matters and do not serve as the attorneys for complainants.

WEC's staff electronically tracked information about individual complaints and regularly informed WEC with relevant information about complaints.

We found that WEC's staff electronically tracked information about individual complaints. Such information included the date a given complaint was received, its ongoing status, the date it was resolved, and how it was resolved. We also found that WEC's staff regularly provided WEC with relevant information about complaints, including responses of individuals accused in the complaints. WEC's staff also recommended actions for WEC to take to resolve the complaints, including recommending that WEC dismiss 11 complaints, refer 3 complaints to district attorneys, deny ballot access based on 6 complaints, allow ballot access based on 2 complaints, and take other actions in response to 2 complaints.

WEC decided how to resolve 24 complaints, including 15 complaints that alleged violations of election laws and 9 ballot access challenges. According to the available minutes and materials from WEC's meetings from January 2020 through June 2021, WEC voted to fully implement its staff's recommendations for 18 of the 24 complaints, partially implement its staff's recommendations for 3 complaints, and reject its staff's recommendations for 3 complaints. In addition, WEC dismissed one complaint that its administrator in consultation with its chairperson had previously dismissed but that the complainant had appealed to WEC.

A total of 25 of 34 complaints about the conduct of election officials and alleged violations of election laws were dismissed.

We used information provided by WEC's staff to determine the resolution as of early-June 2021 of the 34 complaints about the conduct of election officials and alleged violations of election laws. As shown in Table 11:

- 25 complaints were dismissed by WEC or its administrator in consultation with its chairperson,

including because reasonable suspicion or probable cause were not established, or because a violation was determined to be unintentional;

- 6 complaints were not yet resolved;
- 2 complaints were withdrawn by the individuals who had submitted them; and
- 1 complaint was resolved by the administrator in consultation with its chairperson. The decision directed an election official to follow election laws.

Table 11

Resolution of Complaints Filed with WEC Regarding the November 2020 General Election[1]
As of early-June 2021

Resolution	Number	Percentage of Total
Dismissed	25	73.5%
Unresolved	6	17.6
Withdrawn	2	5.9
Decision Issued	1	2.9
Total	**34**	**100.0%**

[1] According to information provided by WEC's staff. Excludes ballot access challenges.

Information provided by WEC's staff for the 11 ballot access challenges included in our review indicated that:

- 7 challenges resulted in a total of 5 candidates being denied ballot access;
- 2 challenges resulted in candidates being provided ballot access;
- 1 challenge was determined not to have been submitted in a timely manner; and
- 1 challenge was withdrawn.

Statutes and administrative rules do not specify the number of days by which WEC must resolve complaints. However, statutes limit the number of days that may pass between specific steps during the complaint process, such as between when WEC's staff receive a complaint and when they forward the complaint to the accused

individual. We found that WEC's staff met these statutorily specified time periods and that the administrator in consultation with the chairperson acted in a timely manner when considering complaints about the conduct of election officials.

Concerns

Individuals can provide election-related concerns to WEC through various methods, including forms on WEC's website.

Election-related concerns are not sworn complaints, and individuals can remain anonymous when providing concerns. Individuals can provide election-related concerns to WEC through various methods, including forms on WEC's website, email messages, and telephone calls.

WEC's staff indicated that they collect election-related concerns to help identify and resolve issues. WEC's staff may take a variety of actions in response to concerns, including requesting additional information, providing individuals with information about submitting sworn complaints, and contacting clerks and other officials about the concerns. WEC's staff indicated that they try to quickly resolve concerns about the accessibility of polling places on Election Day by contacting clerks and poll workers.

Through May 2021, WEC's staff did not track whether or how they had responded to concerns.

Through May 2021, WEC's staff did not systematically track whether or how they had responded to concerns. However, WEC's staff tracked some information about concerns provided through forms on WEC's website, including the text of the concerns and the names and contact information of individuals who submitted concerns, if this information was provided. WEC's staff indicated that they retained email messages conveying concerns but kept these messages in multiple electronic files, and that they did not systematically track or retain information about concerns conveyed through telephone calls. WEC's staff indicated that the large number of concerns they received hindered their ability to track additional information about these concerns and how they responded to them.

WEC's staff provided us with information about 1,521 election-related concerns that had been provided through forms on WEC's website from January 2020 through mid-April 2021. Not all of these concerns pertained to the November 2020 General Election. We reviewed each concern and determined the types of issues discussed in them. Individuals could discuss multiple issues in a given concern.

A total of 611 of the 1,521 concerns provided through forms on WEC's website from January 2020 through mid-April 2021 pertained to absentee ballots.

As shown in Table 12, we found that 611 of the 1,521 concerns (40.2 percent) provided through forms on WEC's website from January 2020 through mid-April 2021 pertained to absentee ballots. Individuals indicated, for example, that they had not received absentee ballots they had requested or had not received them in a timely manner, and they had questions about the security of absentee ballots and whether such ballots were counted.

Table 12

Election-Related Concerns Provided to WEC through Forms on its Website, by Issue[1]
January 2020 through mid-April 2021

Issue	Number	Percentage of Total
Absentee Ballots	611	40.2%
Public Health Crisis	574	37.7
Polling Place Location and Practices	366	24.1
Electioneering or External Group Involvement in Elections	110	7.2
Voter Registration	86	5.7
MyVote Wisconsin Website	82	5.4
Electronic Voting Equipment	34	2.2
Accessibility	28	1.8
Other[2]	119	7.8

[1] According to information WEC's staff provided on 1,521 election-related concerns. Individuals could discuss multiple issues in a given concern.

[2] Includes requests for information from WEC and concerns about WEC's integrity.

According to minutes and materials from WEC's meetings from January 2020 through June 2021, WEC's staff informed WEC about concerns on three occasions. On two of these occasions, WEC's staff informed WEC about the number of concerns that had been provided in a given time period.

Improving Procedures

In report 14-14, we found that GAB's staff did not have written policies for considering complaints and did not track information regarding all complaints.

In report 14-14, we found that GAB's staff did not have written policies for considering complaints and did not track information regarding all complaints. Therefore, we recommended that GAB's staff present written policies for considering complaints to GAB for its approval. We also recommended that GAB's staff maintain complete, centralized information about all complaints received. 2015 Wisconsin Act 118 required WEC to implement the recommendations in report 14-14.

In our current audit, we found that WEC's staff relied on statutes to guide their considerations, as well as administrative rules for considering complaints about the conduct of election officials. We were unable to determine how WEC's staff considered election-related concerns because they did not track such information through May 2021. In June 2021, WEC executed a two-year $93,000 contract with a firm to provide software that is intended, in part, to track election-related concerns and how its staff responded to these

concerns. WEC's staff indicated that they plan to implement this software later in 2021.

Improvements should be made to how election-related complaints and concerns are considered.

Improvements should be made to how election-related complaints and concerns are considered. Because administrative rules for considering complaints alleging violations of election laws are no longer in effect, WEC's staff should work with WEC to promulgate rules for considering such complaints. Administrative rules could, for example, describe the types of information that should be included in complaints and allow a complainant to respond to any information provided to WEC's staff by the subject of a complaint. Promulgating administrative rules allows the Governor and the Legislature to participate in the process of determining how WEC's staff consider complaints, and administrative rules carry the force of law.

WEC's staff should also use the recently purchased software to track information about concerns, including those provided through forms on WEC's website, email messages, and telephone calls. Such information should at a minimum include the types of concerns received and how WEC's staff responded to these concerns. WEC's staff should regularly provide summary information about these concerns to WEC. Doing so will help WEC and staff managers to ensure that staff are taking consistent and appropriate actions, as well as to better understand the scope and breadth of the concerns provided.

☑ Recommendation

We recommend staff of the Wisconsin Elections Commission:

- *work with the Wisconsin Elections Commission to promulgate administrative rules for considering complaints alleging violations of election laws;*
- *use recently purchased software to track election-related concerns and regularly provide summary information about these concerns to the Wisconsin Elections Commission; and*
- *report to the Joint Legislative Audit Committee by March 31, 2022, on their efforts to comply with these recommendations.*

Issue for Legislative Consideration

The Legislature could consider modifying statutes to require WEC to report to it certain information about election-related concerns every six months.

Currently, statutes do not require WEC to report any information to the Legislature about the considerable number of election-related concerns that it receives from individuals. The Legislature could consider modifying statutes to require WEC to report to it certain information about election-related concerns every six months. Such information could include the number of election-related concerns that individuals had provided to WEC, the types of issues addressed in these concerns, and how WEC's staff addressed these concerns.

■■■■

Election Recount Costs

If more than 4,000 votes are cast in an election, statutes permit a candidate trailing by no more than 1.0 percent of the total votes cast to petition for a recount.

If more than 4,000 votes are cast in an election, statutes permit a candidate trailing by no more than 1.0 percent of the total votes cast to petition for a recount. Upon receiving a recount petition, statutes require either clerks or WEC to estimate the costs of the recount. After the November 2016 General Election, a presidential candidate requested a statewide recount. After the November 2020 General Election, a different presidential candidate requested a recount in Dane and Milwaukee counties. In both counties, the estimated recount costs and the actual recount costs increased considerably from 2016 to 2020. In both counties, the actual recount costs in 2016 were lower than the estimated recount costs, and the actual recount costs in 2020 were lower than the estimated recount costs. Statutes do not require WEC to ensure that the estimated costs and the actual costs are reasonable and appropriate. We include two issues for legislative consideration.

If the difference in a vote total exceeds 0.25 percent, statutes require a petitioning candidate to prepay the estimated recount costs before a recount begins. If the actual cost of a recount differs from the estimated cost, a petitioning candidate either owes an additional amount or is refunded the excess amount that had been prepaid. If an election outcome changes because of a recount, the petitioning candidate is not required to pay. On November 18, 2020, a presidential candidate who trailed in the vote total by 0.62 percent filed a petition for a recount in Dane and Milwaukee counties and prepaid WEC $3.0 million. On November 19, 2020, WEC ordered a recount.

Statutes require a recount to be conducted by the county board of canvassers, which includes the county clerk and two qualified electors appointed by the county clerk for two-year terms. One of these two electors must belong to a political party other than the county clerk's

party. A recount must begin no later than 9:00 a.m. on the third day after receipt of a recount order from WEC and be completed no later than 13 days after receipt of a recount order. Milwaukee County completed the recount on November 27, and Dane County completed it on November 29.

Estimated Recount Costs

In anticipation of a statewide recount, WEC provided all county clerks with a template for estimating recount costs.

In anticipation of a possible statewide recount after the November 2020 General Election, WEC advised all county clerks to estimate their recount costs and provided them with a template that:

- suggested allowable cost categories and indicated that certain costs were not reimbursable, including those for alcoholic beverages, traffic citations, and child care;
- included a link to a given county's estimated and actual recount costs in 2016 and indicated that clerks could use this information to estimate recount costs in 2020; and
- included a signature line for a clerk to attest that a county's estimated costs were accurate, reasonable, and necessary.

Although statutes require WEC to prescribe standard forms and procedures for conducting a recount, WEC's staff indicated that county clerks were not required to use the template to estimate recount costs. WEC's staff indicated that WEC interprets this statutory requirement to relate to the recount process, such as how ballots are counted, but not to how clerks should estimate recount costs.

We reviewed the estimated costs that all 72 county clerks provided to WEC for the 2016 and the 2020 recounts and found that these estimated costs:

- increased in 58 counties, including from $6,100 to $45,300 in Juneau County, where the 642.6 percent change was the largest percentage increase among all counties; and
- decreased in 14 counties, including from $141,000 to $20,000 in Pierce County, where the 85.8 percent change was the largest percentage decrease among all counties.

From 2016 to 2020, the estimated cost of the recount increased in Milwaukee and Dane counties.

From 2016 to 2020, the estimated cost of the recount increased by 279.9 percent in Milwaukee County and by 116.1 percent in Dane County, as shown in Table 13. The percentage increase in Milwaukee County was the 12th largest among all counties, and the percentage increase in Dane County was the 32nd largest. For all other counties combined, the estimated cost for the 2020 recount was 69.0 percent greater than the estimated cost for the 2016 recount.

Table 13

Estimated Costs of the Recounts[1]

Recounts Conducted after the November 2016 and November 2020 General Elections

	2016	2020	Percentage Increase
Milwaukee County	$536,700	$2,039,000	279.9%
Dane County	342,800	740,800	116.1

[1] According to information that counties provided to WEC.

Many factors can affect recount costs, including the number of ballots to be recounted. From 2016 to 2020, the number of ballots cast increased by 11.4 percent in Dane County, 4.2 percent in Milwaukee County, and 12.0 percent in all other counties combined. In addition, WEC provided county clerks with guidance on costs that were reasonable to include in 2020 because of the public health emergency. Such costs included additional space rental to allow for social distancing, personal protective equipment, hand sanitizer and masks, and plexiglass dividers, as well as the costs of safely allowing recount observers and livestreaming services if in-person space was limited. In 2020, Milwaukee County included $15,500 for public health emergency–specific items in its estimated costs, and Dane County included $14,500. However, both counties indicated that most types of costs were affected by the public health emergency.

The estimated per-ballot cost of the recount increased from:

- $1.11 in 2016 to $2.15 in 2020 (93.7 percent) in Dane County;
- $1.22 in 2016 to $4.44 in 2020 (263.9 percent) in Milwaukee County; and
- $1.36 in 2016 to $2.05 in 2020 (50.7 percent) in all other counties combined.

WEC's staff indicated that they briefly reviewed the estimated and actual recount cost information that county clerks provided before sending this information to petitioning candidates. WEC's staff indicated that WEC does not believe it has the statutory authority to question the cost information.

We question whether WEC's staff sufficiently reviewed the cost information in 2016 before sending it to the petitioning candidate. We found that WEC's staff:

- informed the petitioning candidate that the recount's estimated cost was $3.5 million, even though counties had provided estimated costs totaling $3.9 million; and
- did not realize the actual cost information provided by Dane County included $25,600 in duplicated costs, which the petitioning candidate subsequently paid.

Actual Recount Costs

In 2016 and 2020, the actual costs of the recount were lower than the estimated costs in Milwaukee and Dane counties.

As shown in Table 14, the actual costs of the recount in 2016 in Milwaukee and Dane counties were lower than the estimated costs, and the actual costs in 2020 in both counties were lower than the estimated costs. For all other counties in 2016, the average estimated cost was $43,100 per county, and the average actual cost was $21,900. Thirteen counties had actual costs that exceeded estimated costs by a total of $14,000.

Table 14

Comparison of Estimated Costs and Actual Costs of Recounts[1]
Recounts Conducted after the November 2016 and November 2020 General Elections

	2016		2020	
County	Estimated Costs	Actual Costs	Estimated Costs	Actual Costs
Milwaukee	$536,700	$271,500	$2,039,000	$1,719,200
Dane	342,800	201,700	740,800	729,700

[1] According to information that counties provided to WEC.

We examined in greater detail the actual costs of the recounts in 2016 and 2020. 2017 Wisconsin Act 120, which was enacted in

November 2017, allowed WEC to include its own recount-related costs in the amounts paid by petitioning candidates. For the 2020 recount, the petitioning candidate paid $6,200 for WEC's costs.

The actual cost of the 2020 recount totaled $2.4 million in Milwaukee and Dane counties.

As shown in Table 15, the actual cost of the 2020 recount totaled $2.4 million for Milwaukee and Dane counties, which was more than five times greater than the $473,100 charged by the two counties for the 2016 recount. From 2016 to 2020:

- Milwaukee County's actual costs increased by 533.3 percent, and its per-ballot costs increased from $0.62 to $3.74; and
- Dane County's actual costs increased by 261.9 percent, and its per-ballot costs increased from $0.65 to $2.12.

Table 15

Actual Costs of the Recounts[1]
Recounts Conducted after the November 2016 and November 2020 General Elections

	2016	2020	Percentage Change
Milwaukee County			
Facilities	$ 7,500	$ 623,000	8,206.7%
Election Systems and Equipment	45,500	499,100	996.9
Staffing	167,200	408,800	144.5
Security	33,900	141,000	315.9
Other[2]	17,300	47,400	174.0
Subtotal	271,500	1,719,200	533.2
Dane County			
Staffing	125,500	279,400	122.6
Election Systems and Equipment	–	151,600	–
Facilities	22,200	144,100	549.1
Security	–	113,000	–
Other[2]	54,000 [3]	41,600	(23.0)
Subtotal	201,700	729,700	261.8
Total	**$473,100**	**$2,449,000**	417.6

[1] According to information that Dane and Milwaukee counties provided to WEC. Excludes $6,200 in WEC's costs in 2020.

[2] Includes supplies and municipal costs.

[3] Includes $25,600 in double-counted costs that the petitioning candidate paid.

We examined the reasons that the actual costs of the recounts in Dane and Milwaukee counties increased from 2016 to 2020. To do so, we reviewed cost information the two counties provided. The two counties did not consistently report similar types of information.

Staffing

Statutes indicate that a board of canvassers may employ individuals to help complete recount work and that these individuals must be paid a reasonable daily compensation or a proportionate hourly rate. WEC's staff indicated that each county determines how much to pay. County staff and municipal employees may also complete recount work.

From 2016 to 2020, Dane County's recount costs for staffing increased from $125,500 to $279,400.

From 2016 to 2020, Dane County's recount costs for staffing increased from $125,500 to $279,400. Information provided by the county indicated that:

- From 2016 to 2020, the total cost of individuals it hired increased from $102,000 to $243,100.
- In 2016, the county paid all individuals it hired $20 per hour. In 2020, it paid 199 individuals $30 per hour, 5 individuals $45 per hour, and 1 individual $60 per hour. The county indicated that hourly rates increased, in part, because of cost of living adjustments and the need to ensure adequate staffing levels during a public health emergency.
- The county paid no overtime to individuals it hired in 2016, but it paid $19,300 for 373.5 hours of overtime to individuals it hired in 2020.
- In 2016, the costs of recount work performed by county staff totaled $21,800, including $7,000 for the county clerk. In 2020, county staff costs totaled $34,900, excluding work performed by the county clerk, for which the county did not seek reimbursement. The county indicated that although it was reimbursed for the costs of staff time, staff did not receive additional compensation for recount work.

From 2016 to 2020, Milwaukee County's recount costs for staffing increased from $167,200 to $408,800.

From 2016 to 2020, Milwaukee County's recount costs for staffing increased from $167,200 to $408,800. Each municipality in the county hired individuals and determined the amounts to pay them. Information provided by the county indicated that:

- The City of Milwaukee paid individuals it hired $15 per hour in 2016 and $23.91 in 2020. It indicated that it increased the hourly pay because of

recruiting difficulties caused, in part, because Dane County paid individuals $30 per hour.

- In 2020, the cities of Milwaukee and West Allis paid individuals $138,500 for 3,691.4 hours of overtime, which accounted for 96.3 percent of all hours reported by these two cities.

- In 2016, the costs of recount work performed by county staff totaled $33,200. In 2020, county staff costs totaled $34,400, including the cost of 64 hours of work performed by the county clerk, for which the county sought reimbursement. The county indicated that although it was reimbursed for the costs of staff time, its staff did not receive additional compensation for recount work.

Facilities

In deciding on a facility in which to conduct a recount, counties consider factors such as accessibility, space, and cost. Facility costs may include rent, parking, and meals.

From 2016 to 2020, Dane County's facility costs increased from $22,200 to $144,100.

From 2016 to 2020, Dane County's facility costs increased from $22,200 to $144,100. Information provided the county indicated that:

- In 2016, the county used the Madison City-County Building to conduct the recount at a cost of $8,000. In 2020, it paid $103,400 to rent space at the Monona Terrace Community and Convention Center. The county indicated that it did not use the City-County Building because it needed more space to allow social distancing for recount workers and observers.

- In 2020, the county considered renting space at the Monona Terrace or the Alliant Energy Center but did not obtain a cost estimate for the Alliant Energy Center. The county indicated that it chose the Monona Terrace because of its proximity to the City-County Building and because the Alliant Energy Center was being used for public health emergency–related purposes.

- The contract with the Monona Terrace required the county to rent space and pay for catered meals for 13 days, which is the statutorily stipulated amount of time to complete a recount. After the county completed its recount in 10 days, it paid a $6,100 cancellation fee and was refunded a portion of the costs of meals it no longer needed.

From 2016 to 2020, Milwaukee County's facility costs increased from $7,500 to $623,000.

From 2016 to 2020, Milwaukee County's facility costs increased from $7,500 to $623,000. Information provided by the county indicated that:

- In 2016, the county used a Milwaukee Election Commission warehouse to conduct the recount and reported no costs. In 2020, it paid $510,400 to rent space at the Wisconsin Center. The county indicated that it did not use the warehouse, in part, because the City of Milwaukee did not make the warehouse available, the county needed more space to allow social distancing, and the Wisconsin Center provided catering and security.

- Before renting space at the Wisconsin Center, the county considered using the Milwaukee County Sports Complex, the Fiserv Forum, and 501 West Michigan Avenue, where the City of Milwaukee had conducted its central count on Election Day.

- The county completed its recount in 8 days, but it paid to rent space at the Wisconsin Center for 12 days, including 2 days when voting equipment and other recount supplies were on-site.

A county may provide meals to individuals helping with a recount. The Department of Administration's (DOA's) guidelines indicate that state employees can be reimbursed up to $10 for lunch and $20 for dinner when traveling for work in the state. Statutes do not limit meal costs for recounts or require counties to follow DOA's meal reimbursement guidelines.

According to information provided by the counties, meal costs were included in the total facility costs in 2020. Information provided indicated:

- From 2016 to 2020, Dane County's meal costs increased from $4,000 to $28,400. The Monona Terrace catered box lunches for $10 per person and dinners for $20 per person.

- From 2016 to 2020, Milwaukee County's meal costs increased from $7,500 to $72,300. The Wisconsin Center catered box lunches for $23 per person but did not provide dinners.

Election Systems and Equipment

From 2016 to 2020, Dane County's election systems and equipment costs increased from $0 to $151,600.

In 2016, Dane County reported no costs for election systems and equipment because it recounted ballots by hand. In 2020, the county reported $151,600 in such costs, in part, because it used four automatic tabulating machines to complete most of the recount. This amount included $9,700 for various costs at Monona Terrace, including four television screens, two document cameras, two laptops, two web cameras, and microphones.

From 2016 to 2020, Milwaukee County's election systems and equipment costs increased from $45,500 to $499,100.

From 2016 to 2020, Milwaukee County's election systems and equipment costs increased from $45,500 to $499,100. Information provided by the county indicated that:

- In 2016, the county counted ballots with four automatic tabulating machines provided by the City of Milwaukee, including two machines rented for $34,400 from the vendor of the machines and two machines provided at no cost by the city. In 2020, the city provided seven machines and charged the county $117,000 for costs associated with wear and tear. This amount was one-half of the amount that the manufacturer would have charged to rent the machines.

- In 2020, a portion of the Wisconsin Center's costs included technology, such as approximately $355,100 for audio-visual production and streaming, electronic systems, and equipment.

Issues for Legislative Consideration

We reviewed whether other midwestern states limit the amount of recount costs that can be charged to petitioning candidates. We found that:

- Minnesota requires each jurisdiction where a recount is conducted to make available at no cost all necessary equipment and facilities; and

- Michigan requires petitioning candidates to pay statutorily predetermined amounts of up to $250 per precinct, regardless of their actual recount costs.

If the Legislature wanted to limit the types of recount costs charged to petitioning candidates, it could modify statutes to require that only certain types of costs could be charged.

If the Legislature wanted to limit the types of recount costs charged to petitioning candidates, it could modify statutes to require that only certain types of costs could be charged. For example, it could stipulate that petitioning candidates not be charged costs associated with facilities, certain types of equipment, or the salaries and fringe benefits of government employees, who may be expected to fulfill at no cost all duties pertaining to administering elections. Similarly, it could stipulate that recounts must occur in government facilities whenever possible, or require counties to show that they rented reasonably priced private facilities. However, circumstances such as a public health emergency could result in counties incurring new and unanticipated types of costs, and taxpayer funds could end up financing a portion of the recount costs that petitioning candidates currently cover.

If the Legislature wanted to limit the total recount costs charged to petitioning candidates, it could modify statutes to determine the amount that could be charged.

If the Legislature wanted to limit the total recount costs charged to petitioning candidates, it could modify statutes to determine the total amount that could be charged. For example, statutes could stipulate an amount per ballot to be recounted, and statutes could stipulate that this amount would increase over time, such as by the rate of inflation. Doing so would ensure a petitioning candidate knew in advance the cost of a recount. However, actual costs could vary considerably among counties, and taxpayer funds could end up financing a portion of the recount costs that petitioning candidates currently cover, particularly if costs increase during circumstances such as a public health emergency.

■ ■ ■ ■

Appendices

Appendix 1

WEC Commissioners, by Appointing Authority

October 2021

Commissioner	Appointing Authority
Marge Bostelmann	Governor
Julie Glancey	Governor
Ann Jacobs	Senate Minority Leader
Dean Knudson	Assembly Speaker
Robert Spindell, Jr.	Senate Majority Leader
Mark Thomsen	Assembly Minority Leader

Appendix 2

Eight Groups Involved with Elections Administration Issues That We Contacted

Disability Rights Wisconsin

League of Wisconsin Municipalities

League of Women Voters of Wisconsin

Wisconsin Counties Association

Wisconsin County Clerks Association

Wisconsin Election Integrity

Wisconsin Municipal Clerks Association

Wisconsin Towns Association

Appendix 3

Municipal Clerks and County Clerks That We Contacted, by County

County	Clerk
Adams	Adams, Town of
	Jackson, Town of
Ashland	Ashland, City of
Barron	Barron County
	Chetek, City of
	Stanfold, Town of
Brown	Allouez, Village of
	Ashwaubenon, Village of
	Bellevue, Village of
	De Pere, City of
	Green Bay, City of
	Hobart, Village of
	Rockland, Town of
	Suamico, Village of
Buffalo	Belvidere, Town of
	Cross, Town of
	Milton, Town of
Burnett	Sand Lake, Town of
	Union, Town of
Calumet	Brillion, City of
	Chilton, Town of
	Harrison, Town of
	New Holstein, City of
Chippewa	Chippewa Falls, City of
	Cornell, City of
	Tilden, Town of
Clark	Hendren, Town of
	Loyal, City of
	Thorp, City of
	Withee, Village of
Columbia	Cambria, Village of
	Lodi, City of
Crawford	Lynxville, Village of

County	Clerk
Dane	Christiana, Town of
	Cottage Grove, Town of
	Dane County
	Deerfield, Town of
	Madison, City of
	Maple Bluff, Village of
	Mount Horeb, Village of
	Oregon, Town of
	Perry, Town of
	Rutland, Town of
	Stoughton, City of
	Sun Prairie, City of
	Verona, City of
	Westport, Town of
Dodge	Chester, Town of
	Dodge County
	Lebanon, Town of
	Rubicon, Town of
Door	Door County
	Egg Harbor, Town of
	Jacksonport, Town of
	Liberty Grove, Town of
Douglas	Superior, City of
Dunn	Colfax, Village of
Eau Claire	Eau Claire, City of
Fond du Lac	Campbellsport, Village of
	Fond du Lac, City of
	Fond du Lac County
	Friendship, Town of
Grant	Bloomington, Town of
	Platteville, City of
Green Lake	Berlin, City of
	Brooklyn, Town of
	Green Lake County

County	Clerk
Jackson	Alma, Town of
	Curran, Town of
Jefferson	Oakland, Town of
	Watertown, City of
Juneau	Juneau County
	Lemonweir, Town of
	Marion, Town of
	New Lisbon, City of
Kenosha	Kenosha, City of
	Kenosha County
	Pleasant Prairie, Village of
	Somers, Town of
	Somers, Village of
Kewaunee	Kewaunee County
La Crosse	La Crosse, City of
	Medary, Town of
Lafayette	Blanchardville, Village of
Langlade	Antigo, City of
Manitowoc	Manitowoc, City of
Marathon	Day, Town of
	Marathon City, Village of
	Marathon County
	Wausau, City of
	Weston, Village of
Marinette	Marinette County
	Niagara, City of
Marquette	Neshkoro, Town of
Menominee	Menominee County
Milwaukee	Franklin, City of
	Greendale, Village of
	Greenfield, City of
	Milwaukee, City of
	Milwaukee County
	Oak Creek, City of
	Shorewood, Village of
	South Milwaukee, City of
	Wauwatosa, City of
	West Allis, City of
	Whitefish Bay, Village of

County	Clerk
Monroe	Sparta, City of
	Wells, Town of
Oconto	Little River, Town of
	Oconto, City of
Outagamie	Grand Chute, Town of
	Little Chute, Village of
	Oneida, Town of
	Outagamie County
Ozaukee	Cedarburg, City of
	Port Washington, City of
Pepin	Durand, City of
	Stockholm, Town of
Pierce	Ellsworth, Town of
	River Falls, City of
Polk	Farmington, Town of
Portage	Sharon, Town of
Price	Price County
Racine	Mount Pleasant, Village of
	North Bay, Village of
Richland	Marshall, Town of
Rock	Beloit, City of
	Janesville, City of
	Johnstown, Town of
	Spring Valley, Town of
Rusk	Grant, Town of
	Willard, Town of
Sawyer	Sawyer County
	Winter, Village of
Shawano	Bartelme, Town of
Sheboygan	Holland, Town of
	Mitchell, Town of
	Random Lake, Village of
	Sheboygan Falls, City of
St. Croix	Baldwin, Village of
	Hudson, City of
	Roberts, Village of
	St. Croix County
	Star Prairie, Town of

County	Clerk
Taylor	Greenwood, Town of
Vernon	Forest, Town of
	Viroqua, City of
Vilas	Lac du Flambeau, Town of
	Vilas County
Walworth	Elkhorn, City of
	Walworth County
	Whitewater, City of
Washington	Barton, Town of
	Erin, Town of
	Germantown, Village of
	Jackson, Town of
	Jackson, Village of
	Richfield, Village of
	Washington County
	West Bend, City of
Waukesha	Brookfield, City of
	Menomonee Falls, Village of
	New Berlin, City of
	Oconomowoc, City of
	Ottawa, Town of
	Pewaukee, City of
Waupaca	Little Wolf, Town of
	Waupaca County
Waushara	Richford, Town of
Winnebago	Algoma, Town of
	Clayton, Town of
	Fox Crossing, Village of
	Menasha, City of
	Neenah, City of
	Oshkosh, City of
	Winnebago County
Wood	Arpin, Town of
	Marshfield, City of
	Wisconsin Rapids, City of

Appendix 4

Review of a Sample of Absentee Ballot Certificates in the November 2020 General Election

This appendix provides an overview of the 14,710 certificates we reviewed in 29 municipalities. We determined the extent to which these certificates had partial witness addresses. For purposes of our analysis, we determined a partial witness address to exclude one or more of the following: street name and number, municipality, state, and zip code. We also determined the extent to which these certificates did not have entire witness addresses, witness signatures, or voter signatures. The following tables present the results of our review.

Descriptions of key terms follow.

Total Certificates is the total number of certificates associated with absentee ballots cast in the November 2020 General Election in a given municipality, according to WisVote data.

Certificates We Reviewed includes the number of certificates we reviewed in a given municipality, the number of certificates that we found to have an issue (e.g., certificates with partial witness addresses), and the percentage of certificates that we found to have an issue (e.g., certificates with partial witness addresses).

Estimated Total Number of Certificates that had a given issue (e.g., certificates with partial witness addresses) presents our low estimate and high estimate of the number of all certificates in a given municipality that had a given issue. Based on statistical approximation, we are 95.0 percent confident that the total number of certificates with a given issue in a municipality is between these low and high estimates. If the certificates we reviewed did not indicate that a given issue occurred in a given municipality, we do not provide estimates for that municipality.

Because we reviewed all or almost all certificates in 8 of the 29 municipalities, we instead provide the actual total number of certificates in a given municipality that had a given issue.

In the City of Sun Prairie, we reviewed a large sample of certificates that we did not select randomly, so we cannot use statistical approximation to estimate the total number of certificates that had a given issue.

Certificates with Partial Witness Addresses[1]

Municipality	Total Certificates	Certificates We Reviewed			Estimated Total Number of Certificates with Partial Witness Addresses[2]		Actual Total Number of Certificates with Partial Witness Addresses
		Number	Number with Partial Witness Addresses	Percentage with Partial Witness Addresses	Low Estimate	High Estimate	
Appleton, City of	24,196	551	15	2.72%	401	1,075	
Bayside, Village of	2,689	521	46	8.83	180	312	
Brookfield, City of	20,923	760	287	37.76	7,195	8,634	
Eau Claire, City of	22,348	469	15	3.20	436	1,165	
Franklin, Town of (Jackson County)	30	30	1	3.33			1
Glendale, City of	7,010	499	1	0.20	3	79	
Green Bay, City of	32,051	485	39	8.04	1,904	3,463	
Greenfield, Town of (La Crosse County)	744	744	66	8.87			66
Highland, Village of	186	186	8	4.30			8
Janesville, City of	22,515	631	27	4.28	666	1,386	
Kekoskee, Village of	162	162	62	38.27			62
Kenosha, City of	30,434	520	3	0.58	60	512	
Ledgeview, Town of (Brown County)	4,297	533	13	2.44	62	178	
Little Suamico, Town of (Oconto County)	1,772	886	67	7.56	107	169	
Loyal, Town of (Clark County)	62	62	11	17.74			11
McFarland, Village of	4,902	541	0	0.0			
Middleton, City of	11,202	507	6	1.18	61	287	
Milwaukee, City of	169,208	597	1	0.17	51	1,596	
Oshkosh, Town of (Winnebago County)	901	899	68	7.56			68
Racine, City of	20,739	506	7	1.38	140	587	
Rib Lake, Village of	139	139	2	1.44			2

Municipality	Total Certificates	Certificates We Reviewed			Estimated Total Number of Certificates with Partial Witness Addresses[2]		Actual Total Number of Certificates with Partial Witness Addresses
		Number	Number with Partial Witness Addresses	Percentage with Partial Witness Addresses	Low Estimate	High Estimate	
Shorewood, Village of	7,947	521	141	27.06%	1,862	2,467	
Shorewood Hills, Village of	1,439	722	14	1.94	17	47	
Sullivan, Village of	146	146	3	2.05			3
Sun Prairie, City of[3]	16,758	1,000	24	2.40			
Verona, City of	7,095	504	13	2.58	108	310	
Waukesha, City of	26,355	563	33	5.86	1,108	2,140	
Wauwatosa, City of	25,508	524	27	5.15	910	1,886	
Whitefish Bay, Village of	8,270	502	22	4.38	241	542	
Totals	**470,028**	**14,710**	**1,022**	6.95			

[1] Certificates did not have one or more address components, including street name and number, municipality, state, and zip code.

[2] Based on statistical approximation, we are 95.0 percent confident that the total number of certificates with partial witness addresses is between the low and high estimates.

[3] Statistical approximation cannot be used to estimate the total number of certificates because we did not randomly select certificates for review.

Certificates without an Entire Witness Address

Municipality	Total Certificates	Certificates We Reviewed			Estimated Total Number of Certificates without an Entire Witness Address[1]		Actual Total Number of Certificates without an Entire Witness Address
		Number	Number without an Entire Witness Address	Percentage without an Entire Witness Address	Low Estimate	High Estimate	
Appleton, City of	24,196	551	0	0.0%			
Bayside, Village of	2,689	521	2	0.38	3	38	
Brookfield, City of	20,923	760	0	0.0			
Eau Claire, City of	22,348	469	0	0.0			
Franklin, Town of (Jackson County)	30	30	0	0.0			0
Glendale, City of	7,010	499	0	0.0			
Green Bay, City of	32,051	485	2	0.41	37	478	
Greenfield, Town of (La Crosse County)	744	744	0	0.0			0
Highland, Village of	186	186	0	0.0			0
Janesville, City of	22,515	631	0	0.0			
Kekoskee, Village of	162	162	0	0.0			0
Kenosha, City of	30,434	520	0	0.0			
Ledgeview, Town of (Brown County)	4,297	533	1	0.19	2	46	
Little Suamico, Town of (Oconto County)	1,772	886	1	0.11	1	12	
Loyal, Town of (Clark County)	62	62	4	6.45			4
McFarland, Village of	4,902	541	0	0.0			
Middleton, City of	11,202	507	0	0.0			
Milwaukee, City of	169,208	597	0	0.0			
Oshkosh, Town of (Winnebago County)	901	899	0	0.0			0
Racine, City of	20,739	506	1	0.20	8	231	
Rib Lake, Village of	139	139	1	0.72			1

Municipality	Total Certificates	Certificates We Reviewed			Estimated Total Number of Certificates without an Entire Witness Address[1]		Actual Total Number of Certificates without an Entire Witness Address
		Number	Number without an Entire Witness Address	Percentage without an Entire Witness Address	Low Estimate	High Estimate	
Shorewood, Village of	7,947	521	0	0.0%			
Shorewood Hills, Village of	1,439	722	0	0.0			
Sullivan, Village of	146	146	1	0.68			1
Sun Prairie, City of[2]	16,758	1,000	0	0.0			
Verona, City of	7,095	504	1	0.20	3	80	
Waukesha, City of	26,355	563	0	0.0			
Wauwatosa, City of	25,508	524	0	0.0			
Whitefish Bay, Village of	8,270	502	1	0.20	3	93	
Totals	**470,028**	**14,710**	**15**	0.10			

[1] Based on statistical approximation, we are 95.0 percent confident that the total number of certificates without an entire witness address is between the low and high estimates.

[2] Statistical approximation cannot be used to estimate the total number of certificates because we did not randomly select certificates for review.

Certificates without a Witness Signature

Municipality	Total Certificates	Certificates We Reviewed			Estimated Total Number of Certificates without a Witness Signature[1]		Actual Total Number of Certificates without a Witness Signature
		Number	Number without a Witness Signature[2]	Percentage without a Witness Signature	Low Estimate	High Estimate	
Appleton, City of	24,196	551	0	0.0%			
Bayside, Village of	2,689	521	0	0.0			
Brookfield, City of	20,923	760	0	0.0			
Eau Claire, City of	22,348	469	1	0.21	9	268	
Franklin, Town of (Jackson County)	30	30	0	0.0			0
Glendale, City of	7,010	499	1	0.20	3	79	
Green Bay, City of	32,051	485	0	0.0			
Greenfield, Town of (La Crosse County)	744	744	0	0.0			0
Highland, Village of	186	186	0	0.0			0
Janesville, City of	22,515	631	2	0.32	20	259	
Kekoskee, Village of	162	162	0	0.0			0
Kenosha, City of	30,434	520	1	0.19	11	329	
Ledgeview, Town of (Brown County)	4,297	533	0	0.0			
Little Suamico, Town of (Oconto County)	1,772	886	0	0.0			
Loyal, Town of (Clark County)	62	62	0	0.0			0
McFarland, Village of	4,902	541	0	0.0			
Middleton, City of	11,202	507	0	0.0			
Milwaukee, City of	169,208	597	0	0.0			
Oshkosh, Town of (Winnebago County)	901	899	0	0.0			0
Racine, City of	20,739	506	0	0.0			
Rib Lake, Village of	139	139	1	0.72			1

Municipality	Total Certificates	Certificates We Reviewed			Estimated Total Number of Certificates without a Witness Signature[1]		Actual Total Number of Certificates without a Witness Signature
		Number	Number without a Witness Signature[2]	Percentage without a Witness Signature	Low Estimate	High Estimate	
Shorewood, Village of	7,947	521	0	0.0%			
Shorewood Hills, Village of	1,439	722	0	0.0			
Sullivan, Village of	146	146	1	0.68			1
Sun Prairie, City of[3]	16,758	1,000	0	0.0			
Verona, City of	7,095	504	0	0.0			
Waukesha, City of	26,355	563	0	0.0			
Wauwatosa, City of	25,508	524	0	0.0			
Whitefish Bay, Village of	8,270	502	1	0.20	3	93	
Totals	**470,028**	**14,710**	**8**	0.05			

[1] Based on statistical approximation, we are 95.0 percent confident that the total number of certificates without a witness signature is between the low and high estimates.

[2] Individuals who returned five of the eight certificates without a witness signature voted in-person absentee, which typically involves clerk staff writing the witness signature.

[3] Statistical approximation cannot be used to estimate the total number of certificates because we did not randomly select certificates for review.

Certificates without a Voter Signature

Municipality	Total Certificates	Certificates We Reviewed			Estimated Total Number of Certificates without a Voter Signature[1]		Actual Total Number of Certificates without a Voter Signature
		Number	Number without a Voter Signature	Percentage without a Voter Signature	Low Estimate	High Estimate	
Appleton, City of	24,196	551	0	0.0%			
Bayside, Village of	2,689	521	0	0.0			
Brookfield, City of	20,923	760	0	0.0			
Eau Claire, City of	22,348	469	1	0.21	9	268	
Franklin, Town of (Jackson County)	30	30	0	0.0			0
Glendale, City of	7,010	499	0	0.0			
Green Bay, City of	32,051	485	0	0.0			
Greenfield, Town of (La Crosse County)	744	744	0	0.0			0
Highland, Village of	186	186	0	0.0			0
Janesville, City of	22,515	631	2	0.32	20	259	
Kekoskee, Village of	162	162	0	0.0			0
Kenosha, City of	30,434	520	0	0.0			
Ledgeview, Town of (Brown County)	4,297	533	0	0.0			
Little Suamico, Town of (Oconto County)	1,772	886	0	0.0			
Loyal, Town of (Clark County)	62	62	0	0.0			0
McFarland, Village of	4,902	541	0	0.0			
Middleton, City of	11,202	507	0	0.0			
Milwaukee, City of	169,208	597	0	0.0			
Oshkosh, Town of (Winnebago County)	901	899	0	0.0			0
Racine, City of	20,739	506	0	0.0			
Rib Lake, Village of	139	139	0	0.0			0

Municipality	Total Certificates	Certificates We Reviewed			Estimated Total Number of Certificates without a Voter Signature[1]		Actual Total Number of Certificates without a Voter Signature
		Number	Number without a Voter Signature	Percentage without a Voter Signature	Low Estimate	High Estimate	
Shorewood, Village of	7,947	521	0	0.0%			
Shorewood Hills, Village of	1,439	722	0	0.0			
Sullivan, Village of	146	146	0	0.0			0
Sun Prairie, City of[2]	16,758	1,000	0	0.0			
Verona, City of	7,095	504	0	0.0			
Waukesha, City of	26,355	563	0	0.0			
Wauwatosa, City of	25,508	524	0	0.0			
Whitefish Bay, Village of	8,270	502	0	0.0			
Totals	**470,028**	**14,710**	**3**	0.02			

[1] Based on statistical approximation, we are 95.0 percent confident that the total number of certificates without a voter signature is between the low and high estimates.

[2] Statistical approximation cannot be used to estimate the total number of certificates because we did not randomly select certificates for review.

Appendix 5

319 Municipalities for Which We Reviewed Election Day Forms, by County

County	Municipality
Adams	Big Flats, Town of
	Colburn, Town of
	Friendship, Village of
	New Haven, Town of
Barron	Barron, Town of
	Cameron, Village of
	Cumberland, Town of
	Haugen, Village of
	Prairie Farm, Village of
	Turtle Lake, Village of
Bayfield	Barksdale, Town of
	Hughes, Town of
	Mason, Village of
Brown	Ashwaubenon, Village of
	Howard, Village of
	Lawrence, Town of
	Wrightstown, Village of
Buffalo	Canton, Town of
	Maxville, Town of
Burnett	Meenon, Town of
	Roosevelt, Town of
	Sand Lake, Town of
	Scott, Town of
	Siren, Town of
	Wood River, Town of
Calumet	Brillion, City of
	Potter, Village of
	Stockbridge, Village of
Chippewa	Anson, Town of
	Arthur, Town of
	Bloomer, City of
	Edson, Town of
	New Auburn, Village of

County	Municipality
Clark	Beaver, Town of
	Dewhurst, Town of
	Hewett, Town of
	Mentor, Town of
	Neillsville, City of
	Sherwood, Town of
	Warner, Town of
	York, Town of
Columbia	Lodi, City of
	Lodi, Town of
	Friesland, Village of
	Marcellon, Town of
	Newport, Town of
	West Point, Town of
	Wyocena, Town of
Crawford	Eastman, Town of
	Freeman, Town of
	Marietta, Town of
	Mount Sterling, Village of
	Soldiers Grove, Village of
	Steuben, Village of
Dane	Bristol, Town of
	Cottage Grove, Village of
	Cross Plains, Town of
	Dane, Town of
	DeForest, Village of
	Dunn, Town of
	Oregon, Town of
	Vermont, Town of
	Verona, City of
	York, Town of

County	Municipality
Dodge	Beaver Dam, Town of
	Calamus, Town of
	Clyman, Village of
	Fox Lake, Town of
	Herman, Town of
	Iron Ridge, Village of
	LeRoy, Town of
	Reeseville, Village of
Door	Ephraim, Village of
	Sister Bay, Village of
Douglas	Amnicon, Town of
	Highland, Town of
	Lakeside, Town of
	Maple, Town of
	Parkland, Town of
Dunn	Colfax, Town of
	Peru, Town of
	Weston, Town of
Eau Claire	Clear Creek, Town of
	Eau Claire, City of
	Lincoln, Town of
Florence	Commonwealth, Town of
	Fern, Town of
	Florence, Town of
Fond du Lac	Byron, Town of
	Campbellsport, Village of
	Eden, Village of
	Eldorado, Town of
	Lamartine, Town of
	Marshfield, Town of
	Ripon, City of
Forest	Alvin, Town of
	Blackwell, Town of
	Freedom, Town of
	Popple River, Town of

County	Municipality
Grant	Bagley, Village of
	Boscobel, Town of
	Castle Rock, Town of
	Cuba City, City of
	Hazel Green, Village of
	Lancaster, City of
	Little Grant, Town of
	Millville, Town of
	Montfort, Village of
	Mount Hope, Town of
	Mount Ida, Town of
	Platteville, Town of
	Wyalusing, Town of
Green	Cadiz, Town of
	York, Town of
Green Lake	St. Marie, Town of
Iowa	Clyde, Town of
	Eden, Town of
	Linden, Village of
	Mifflin, Town of
	Pulaski, Town of
Jackson	Black River Falls, City of
	City Point, Town of
	Garfield, Town of
	Melrose, Town of
	Taylor, Village of
Juneau	Germantown, Town of
	Kildare, Town of
	Kingston, Town of
	Lemonweir, Town of
	Marion, Town of
	Wonewoc, Village of
Kenosha	Somers, Village of
Kewaunee	Ahnapee, Town of
La Crosse	Hamilton, Town of
	Shelby, Town of

County	Municipality
Lafayette	Argyle, Village of
	Benton, Town of
	Blanchard, Town of
	Blanchardville, Village of
	Elk Grove, Town of
	Fayette, Town of
	Gratiot, Town of
	Shullsburg, City of
Langlade	Antigo, Town of
	Elcho, Town of
	Evergreen, Town of
	Norwood, Town of
Lincoln	Bradley, Town of
	Harrison, Town of
	Merrill, Town of
	Pine River, Town of
	Rock Falls, Town of
	Scott, Town of
Manitowoc	Gibson, Town of
	Maple Grove, Town of
	Mishicot, Village of
	Rockland, Town of
Marathon	Cassel, Town of
	Eau Pleine, Town of
	Franzen, Town of
	Green Valley, Town of
	Hewitt, Town of
	Kronenwetter, Village of
	Maine, Village of
	Marathon, Town of
	Marathon City, Village of
	Reid, Town of
	Schofield, City of
	Spencer, Town of
	Spencer, Village of
	Wausau, Town of

County	Municipality
Marinette	Athelstane, Town of
	Coleman, Village of
	Crivitz, Village of
	Lake, Town of
	Niagara, City of
	Wagner, Town of
Marquette	Montello, City of
	Neshkoro, Village of
	Newton, Town of
Menominee	Menominee, Town of
Milwaukee	Bayside, Village of
	Greendale, Village of
	Wauwatosa, City of
Monroe	Warrens, Village of
Onconto	Lena, Village of
	Little River, Town of
Oneida	Little Rice, Town of
	Monico, Town of
	Newbold, Town of
	Schoepke, Town of
Outagamie	Dale, Town of
	Deer Creek, Town of
	Kimberly, Village of
	Seymour, City of
	Seymour, Town of
Ozaukee	Belgium, Village of
Pepin	Frankfort, Town of
	Pepin, Town of
	Waterville, Town of
Pierce	Ellsworth, Village of
	Elmwood, Village of
	Gilman, Town of
	Maiden Rock, Village of
	Trenton, Town of
	Union, Town of

County	Municipality
Polk	Balsam Lake, Village of
	Clayton, Town of
	Clear Lake, Village of
	Georgetown, Town of
	Johnstown, Town of
	Laketown, Town of
	St. Croix Falls, City of
	Sterling, Town of
Portage	Almond, Village of
	Junction City, Village of
	Sharon, Town of
	Stevens Point, City of
Price	Catawba, Village of
	Fifield, Town of
	Hill, Town of
	Knox, Town of
	Park Falls, City of
	Worcester, Town of
Racine	Waterford, Town of
Richland	Richland Center, City of
	Richwood, Town of
	Sylvan, Town of
Rock	Fulton, Town of
	Spring Valley, Town of
Rusk	Glen Flora, Village of
	Grow, Town of
	Hubbard, Town of
	Ingram, Village of
	Murry, Town of
	South Fork, Town of
	Strickland, Town of
	Stubbs, Town of
	Washington, Town of
Sauk	Dellona, Town of
	Fairfield, Town of
	Lake Delton, Village of
	La Valle, Town of
	Loganville, Village of
	Washington, Town of

County	Municipality
Sawyer	Ojibwa, Town of
	Radisson, Village of
	Round Lake, Town of
	Weirgor, Town of
	Winter, Village of
Shawano	Aniwa, Village of
	Hartland, Town of
	Lessor, Town of
	Richmond, Town of
	Shawano, City of
	Wittenberg, Town of
	Wittenberg, Village of
Sheboygan	Cascade, Village of
	Elkhart Lake, Village of
	Oostburg, Village of
	Plymouth, Town of
	Sheboygan, City of
St. Croix	Cylon, Town of
	Eau Galle, Town of
	Forest, Town of
	Richmond, Town of
	Roberts, Village of
	Star Prairie, Village of
	Warren, Town of
Taylor	Chelsea, Town of
	Deer Creek, Town of
	Gilman, Village of
	Medford, City of
	Stetsonville, Village of
	Taft, Town of
Trempealeau	Eleva, Village of
	Trempealeau, Town of
	Trempealeau, Village of
Vernon	Bergen, Town of
	Coon, Town of
	Forest, Town of
	Franklin, Town of
	Greenwood, Town of
	Ontario, Village of
	Stark, Town of

County	Municipality
Vilas	Land O' Lakes, Town of
	Lincoln, Town of
Walworth	Fontana, Village of
	Lake Geneva, City of
Washburn	Brooklyn, Town of
	Minong, Town of
	Minong, Village of
	Spooner, Town of
	Springbrook, Town of
	Stinnett, Town of
	Stone Lake, Town of
Washington	Kewaskum, Town of
Waukesha	Brookfield, City of
	Eagle, Town of
	Eagle, Village of
	Elm Grove, Village of
	Genesee, Town of
	Lannon, Village of
	Muskego, City of
	Nashotah, Village of
	New Berlin, City of
	Oconomowoc Lake, Village of
Waupaca	Bear Creek, Town of
	Dupont, Town of
	Fremont, Town of
	Matteson, Town of
Waushara	Warren, Town of
Winnebago	Black Wolf, Town of
	Wolf River, Town of
Wood	Arpin, Town of
	Cranmoor, Town of
	Hewitt, Village of
	Marshfield, Town of
	Saratoga, Town of

Appendix 6

Review of a Sample of Electronic Voting Equipment Test Results

Tests Conducted by Municipal Clerks before the November 2020 General Election

Municipal clerks conducted statutorily required tests of electronic voting equipment before the November 2020 General Election. This appendix provides an overview of the pre-election test results we requested from 29 municipalities.

Descriptions of key terms follow.

Pre-Election Tests Conducted by Clerks within 10 Days before the General Election indicates the number of test results that we examined in each municipality, as well as the number and percentage of test results that we found municipal clerks had conducted within 10 days before the General Election, as statutorily required. We examined a total of 175 test results for this analysis. In some municipalities, we examined all test results. In others, we examined a sample of test results.

Pre-Election Tests That Accurately Counted Votes indicates the number of test results that we examined in each municipality, as well as the number and percentage of test results that we found had accurately counted votes for the presidential contest. We examined a total of 60 test results for this analysis.

The following tables present the results of our review.

Pre-Election Tests Conducted by Clerks within 10 Days before the General Election

Municipality	Number of Tests We Reviewed	Number of Reviewed Tests Conducted within 10 Days Before the Election	Percentage of Reviewed Tests Conducted within 10 Days Before the Election
Appleton, City of [1]	–	–	–
Bayside, Village of	1	0	0.0%
Brookfield, City of	34	34	100.0
Eau Claire, City of	23	1	4.3
Franklin, Town of (Jackson County)	1	1	100.0
Glendale, City of	1	0	0.0
Green Bay, City of	44	8	18.2
Greenfield, Town of (La Crosse County)	1	1	100.0
Highland, Village of	1	1	100.0
Janesville, City of	5	5	100.0
Kekoskee, Village of	1	0	0.0
Kenosha, City of	23	1	4.3
Ledgeview, Town of (Brown County)	2	2	100.0
Little Suamico, Town of (Oconto County)	2	2	100.0
Loyal, Town of (Clark County)	1	1	100.0
McFarland, Village of	6	6	100.0
Middleton, City of [1]	–	–	–
Milwaukee, City of	1	0	0.0
Oshkosh, Town of (Winnebago County)	2	2	100.0
Racine, City of [1]	–	–	–
Rib Lake, Village of	1	1	100.0
Shorewood, Village of	1	0	0.0
Shorewood Hills, Village of	1	1	100.0
Sullivan, Village of	1	1	100.0
Sun Prairie, City of	16	16	100.0
Verona, City of	4	4	100.0
Waukesha, City of [1]	–	–	–
Wauwatosa, City of	1	0	0.0
Whitefish Bay, Village of	1	0	0.0
Totals	**175**	**88**	

[1] This municipality did not provide us with any pre-election test results.

Pre-Election Tests That Accurately Counted Votes

Municipality	Number of Tests We Reviewed	Number of Reviewed Tests That Accurately Counted Votes	Percentage of Reviewed Tests That Accurately Counted Votes
Appleton, City of [1]	–	–	–
Bayside, Village of	1	1	100.0%
Brookfield, City of	8	8	100.0
Eau Claire, City of	12	12	100.0
Franklin, Town of (Jackson County)	1	1	100.0
Glendale, City of	1	1	100.0
Green Bay, City of [2]	8	7	87.5
Greenfield, Town of (La Crosse County)	1	1	100.0
Highland, Village of	1	1	100.0
Janesville, City of	5	5	100.0
Kekoskee, Village of	1	1	100.0
Kenosha, City of	1	1	100.0
Ledgeview, Town of (Brown County)	2	2	100.0
Little Suamico, Town of (Oconto County)	2	2	100.0
Loyal, Town of [3] (Clark County)	–	–	–
McFarland, Village of	2	2	100.0
Middleton, City of [1]	–	–	–
Milwaukee, City of	1	1	100.0
Oshkosh, Town of (Winnebago County)	2	2	100.0
Racine, City of [1]	–	–	–
Rib Lake, Village of	1	1	100.0
Shorewood, Village of	1	1	100.0
Shorewood Hills, Village of	1	1	100.0
Sullivan, Village of	1	1	100.0
Sun Prairie, City of	2	2	100.0
Verona, City of	3	3	100.0
Waukesha, City of [1]	–	–	–
Wauwatosa, City of	1	1	100.0
Whitefish Bay, Village of	1	1	100.0
Totals	**60**	**59**	

[1] This municipality did not provide us with any pre-election test results.

[2] One pre-election test result included insufficient documentation, which prevented us from determining whether the equipment had accurately counted the votes for presidential candidates.

[3] This municipality provided us with incomplete pre-election test results.

Appendix 7

Report Recommendations, by Chapter

We recommend staff of the Wisconsin Elections Commission report to the Joint Legislative Audit Committee by March 31, 2022, on their efforts to implement our report recommendations.

Training *(p. 9)*

We recommend staff of the Wisconsin Elections Commission:

- work with the Wisconsin Elections Commission to modify ch. EL 12, Wis. Adm. Code, to reflect current statutory requirements for elections *(p. 10)*.

We recommend staff of the Wisconsin Elections Commission:

- work with the Wisconsin Elections Commission to modify ch. EL 12.02 (7), Wis. Adm. Code, to specify how the governing bodies of municipalities will be notified when municipal clerks do not report having completed training required by administrative rules *(p. 13)*; and
- consistently comply with administrative rules *(p. 13)*.

We recommend staff of the Wisconsin Elections Commission:

- work with the Wisconsin Elections Commission to promulgate statutorily required administrative rules prescribing the contents of training that municipal clerks provide to special voting deputies and election inspectors *(p. 17)*.

Maintenance of Voter Registration Records *(p. 19)*

We recommend staff of the Wisconsin Elections Commission:

- before January 1, 2022, work with the Wisconsin Elections Commission to execute with the Department of Transportation a new written data-sharing agreement that includes provisions for verifying the information provided by individuals who register to vote by all methods and that specifies the procedures for verifying this information *(p. 24)*;

- establish a system to regularly review and update the data-sharing agreement *(p. 24)*; and

- comply with statutes by working with the Department of Transportation to obtain the electronic signatures of individuals who register online to vote, or request that the Legislature modify the statutory requirement that the Wisconsin Elections Commission obtain them *(p. 24)*.

We recommend staff of the Wisconsin Elections Commission:

- improve how they identify potential duplicate voter registration records in WisVote by comparing driver's license and state identification card numbers of all registered voters each night *(p. 25)*.

We recommend staff of the Wisconsin Elections Commission:

- before January 1, 2022, work with the Wisconsin Elections Commission to execute a new written data-sharing agreement with the Department of Health Services *(p. 28)*; and

- establish a system to regularly review and update the data-sharing agreement *(p. 28)*.

We recommend staff of the Wisconsin Elections Commission:

- before January 1, 2022, work with the Wisconsin Elections Commission to execute a new data-sharing agreement with the Department of Corrections *(p. 30)*; and

- establish a system to regularly review and update the data-sharing agreement *(p. 30)*.

We recommend staff of the Wisconsin Elections Commission:

- work with the Wisconsin Elections Commission to establish a schedule for regularly obtaining each type of data available from the Electronic Registration Information Center and a plan for acting on these data *(p. 34)*.

Absentee Ballots *(p. 37)*

We recommend staff of the Wisconsin Elections Commission:

- ensure that the absentee ballot certificates made available to municipalities comply with statutes by requiring witnesses to print their names *(p. 45)*;

- provide municipal clerks with additional training on the statutory requirement to initial absentee ballot certificates in certain situations *(p. 45)*; and

- promulgate administrative rules to allow municipal clerks to correct or add missing witness address information to absentee ballot certificates, if the Wisconsin Elections Commission believes municipal clerks should be permitted to take such actions *(p. 45)*.

We recommend staff of the Wisconsin Elections Commission:

- promulgate administrative rules to permit municipal clerks to establish drop boxes where individuals can return absentee ballots, if the Wisconsin Elections Commission believes municipal clerks should be permitted to establish drop boxes *(p. 48)*.

We recommend staff of the Wisconsin Elections Commission:

- promulgate administrative rules to specify the situations when municipal clerks should not send special voting deputies to residential care facilities and qualified retirement homes, if the Wisconsin Elections Commission believes municipal clerks should be permitted to take alternative actions in these situations *(p. 53)*.

Ballot Processing *(p. 55)*

We recommend staff of the Wisconsin Elections Commission:

- retract their statutorily noncompliant written guidance that indicates municipal clerks may adjourn before counting all ballots as a result of inevitable circumstances *(p. 61)*; and

- promulgate administrative rules to allow municipal clerks to adjourn in certain circumstances before completing ballot counting, if the Wisconsin Elections Commission believes municipal clerks should be allowed to adjourn in these circumstances *(p. 61)*.

We recommend staff of the Wisconsin Elections Commission:

- work with the Wisconsin Elections Commission to retract the statutorily noncompliant written guidance for establishing polling places *(p. 62)*; and

- promulgate administrative rules to specify the circumstances when municipal clerks can relocate polling places without approval from municipal governing bodies, if the Wisconsin Elections Commission believes municipal clerks should be allowed to relocate polling places in these circumstances *(p. 63)*.

We recommend staff of the Wisconsin Elections Commission:

- take additional actions to improve ballot processing in future elections, such as providing additional training to clerks *(p. 65)*.

Electronic Voting Equipment *(p. 67)*

We recommend staff of the Wisconsin Elections Commission:

- provide additional training to municipal clerks on completing the statutorily required pre-election tests of electronic voting equipment *(p. 73)*.

We recommend staff of the Wisconsin Elections Commission:

- provide training to municipal clerks on reviewing Election Day forms after each election and investigating relevant issues, including those related to tamper-evident seals *(p. 74)*.

We recommend staff of the Wisconsin Elections Commission:

- work with the Wisconsin Elections Commission to promulgate statutorily required administrative rules for helping to ensure the security of software components in approved electronic voting equipment *(p. 78)*.

Post-Election Audit *(p. 79)*

We recommend staff of the Wisconsin Elections Commission:

- ensure equipment vendors provide additional training to municipal clerks on ensuring that ballots are counted accurately when paper jams occur in electronic voting equipment *(p. 83)*.

We recommend staff of the Wisconsin Elections Commission:

- comply with statutes by calculating an error rate for each type of electronic voting equipment used in each General Election *(p. 84)*.

Complaints and Concerns Filed with WEC *(p. 93)*

We recommend staff of the Wisconsin Elections Commission:

- work with the Wisconsin Elections Commission to promulgate administrative rules for considering complaints alleging violations of election laws *(p. 99)*; and

- use recently purchased software to track election-related concerns and regularly provide summary information about these concerns to the Wisconsin Elections Commission *(p. 99)*.

Appendix 8

Legislative Considerations, by Chapter

Training *(p. 9)*

Currently, statutes require municipal clerks to attend training at least once every two years, and WEC's administrative rules require clerks to complete three hours of training in order to receive initial certification for the two-year period in which the training is received. However, statutes and administrative rules do not specify when a new clerk must complete the training for initial certification, and they do not require clerks to be certified before administering an election for the first time. As a result, a clerk could administer an election before having completed the initial training. The Legislature could consider modifying statutes to require clerks to complete the initial training before administering an election. Statutes could exempt from this training requirement those individuals who became clerks only shortly before an election *(p. 13)*.

Currently, statutes do not require individuals to inform WEC of the dates they began working as municipal clerks, and WEC's staff indicated that they are not consistently informed of these dates. The Legislature could consider modifying statutes to require a municipal governing body to notify WEC within 30 days when there is turnover in the clerk position. If WEC were better informed, it could more accurately track whether clerks completed all required training *(p. 13)*.

Maintenance of Voter Registration Records *(p. 19)*

As noted, DOT currently provides information that does not indicate precisely why a given non-match occurred because DOT does not provide WEC with any personally identifiable information. The Legislature could consider modifying statutes to require that DOT provide additional information to WEC when DOT attempts to verify the personally identifiable information provided by registrants. For example, statutes could be modified to require DOT to provide WEC with the names, dates of birth, and driver's license or state identification card numbers for individuals whose information did not match. WEC's staff and clerks we contacted indicated that this additional information would help them to identify and correct errors in voter registration records, such as misspelled names and typos *(p. 24)*.

Currently, statutes do not require WEC to obtain and use ERIC data. The Legislature could consider modifying statutes to require WEC to regularly obtain ERIC data and use them to improve the accuracy and completeness of WisVote. For example, statutes could be modified to require WEC to regularly obtain every three or six months ERIC data for registered Wisconsin voters who may have moved to and registered to vote in other states, who

may have voted in Wisconsin and other states, and who may have died in other states *(p. 34)*.

Absentee Ballots *(p. 37)*

As noted, statutes do not define the components of a witness address that a certificate must contain, such as a street name and number, municipality, state, and zip code. The Legislature could consider modifying statutes to specify the particular address components that a witness must provide on a certificate. For example, witnesses could be required to provide, at a minimum, street names and numbers, as well as their municipalities. Such a definition would allow an absentee ballot to be counted if a witness address excluded a state and a zip code *(p. 45)*.

The Legislature could consider modifying statutes to clarify the extent to which municipal clerks are permitted themselves to correct errors in witness addresses or add missing witness address information. As noted, statutes allow a clerk to return a ballot and its certificate if an individual is able to correct an improperly completed certificate and return the ballot in time for it to be counted on Election Day, but statutes do not otherwise permit or prohibit clerks from correcting errors in witness addresses or adding missing witness address information *(p. 45)*.

As noted, statutes require a certificate to include the signature of the individual who cast the ballot. The Legislature could consider modifying statutes to require municipal clerks to verify the signatures of individuals who cast absentee ballots. In doing so, it could specify the documents that clerks should use to verify these signatures, such as voter registration forms and driver's licenses, and the methods that clerks should use to verify these signatures, such as examining the writing slant, letter spacing, and letter shapes. In addition, it could require clerks to be trained on how to verify signatures *(p. 46)*.

The Legislature could consider modifying statutes to clarify whether individuals are allowed to return absentee ballots to drop boxes. Some individuals believe that statutes allow absentee ballots to be returned to drop boxes or in person to clerk staff at locations other than a clerk's office, regardless of whether a municipal governing body established such locations. They believe that these actions are statutorily allowable because individuals requested ballots by statutorily allowable methods, the drop boxes were established by clerks, and clerk staff collected the ballots. Other individuals believe that statutes do not allow absentee ballots to be returned through drop boxes or to clerk staff at locations other than those designated by a municipal governing body *(p. 49)*.

Currently, statutes require municipal clerks to attempt to send special voting deputies to residential care facilities and qualified retirement homes, regardless of the circumstances. During a public health or other emergency, clerks and special voting deputies may risk disenfranchising individuals

living in such facilities and homes if they cannot obtain entry. The Legislature could consider modifying statutes to prescribe circumstances when clerks are not required to send special voting deputies to such facilities and homes, as well as the procedures clerks must follow in mailing and considering absentee ballots in such circumstances. In September 2021, WEC voted to request that the Governor categorize special voting deputies as essential visitors, which it indicated would allow the deputies entry into facilities and homes during a public health emergency *(p. 54)*.

Ballot Processing *(p. 55)*

The Legislature could consider modifying statutes to specify the actions and responsibilities for consultants at polling places and central count locations on Election Day. For example, statutes could specify the particular actions that consultants are permitted to take, as well as the responsibilities that they are allowed to assume while helping municipal clerks to administer elections *(p. 60)*.

The Legislature could consider modifying statutes to allow new polling places to be quickly established in certain situations, such as in a public health emergency or if a fire or a natural disaster were to damage a polling place to the extent that it could not be used on Election Day. Statutes could specify the situations, if any, in which a municipal clerk could establish polling places without approval from a municipal governing body. For example, a clerk could be given the authority to establish a new polling place for one election if certain types of situations occurred shortly before Election Day. Doing so would help to prevent individuals from being disenfranchised if a polling place were closed shortly before Election Day and insufficient time remained for a municipal governing body to establish a new polling place *(p. 63)*.

Electronic Voting Equipment *(p. 67)*

Statutes require municipal clerks to notify WEC's administrator if they adopt and purchase a new or different type of electronic voting equipment. When municipalities rent equipment, such as to count absentee ballots at central count locations during elections at which many individuals are expected to vote, statutes do not require clerks to notify WEC's administrator. The Legislature could consider modifying statutes to require clerks to notify WEC's administrator if they rent electronic voting equipment. Doing so would allow WEC's administrator, and therefore WEC, to know that all equipment used in the state has been approved by WEC *(p. 70)*.

The Legislature could consider modifying statutes to explicitly require materials related to the pre-election tests of electronic voting equipment to be retained for 22 months after a federal election. Doing so would ensure that these pre-election test materials, which indicate whether electronic voting equipment counted ballots accurately, are retained for the same

period of time as other election-related materials such as ballots and applications for absentee ballots *(p. 75)*.

Post-Election Audit *(p. 79)*

As noted, statutes require WEC to take remedial action if the error rate found in electronic voting equipment exceeds the federal standards that were in effect on October 29, 2002, which was one vote per 500,000 ballot positions. We found that these standards were updated in 2015 to specify that the maximum acceptable error rate is 1 vote per 125,000 contests counted by a given type of equipment. Calculating the error rate based on the number of contests, rather than the number of ballot positions, is more straightforward because ballot positions may vary within and among municipalities, depending on the number of candidates in each contest. The Legislature could consider modifying statutes to reflect the current federal standards for an acceptable equipment error rate *(p. 85)*.

The Legislature could consider modifying statutes to require WEC to conduct risk-limiting post-election audits. Such audits are intended to determine voter intent and determine the validity of the election results, which may be preferable to the current audits that confirm whether the equipment counted ballots according to how it was programmed. As noted, one type of equipment was programmed in such a way that it counted ballot creases as votes in some counties during the November 2020 General Election *(p. 86)*.

Complaints and Concerns Filed with WEC *(p. 93)*

Currently, statutes do not require WEC to report any information to the Legislature about the considerable number of election-related concerns that it receives from individuals. The Legislature could consider modifying statutes to require WEC to report to it certain information about election-related concerns every six months. Such information could include the number of election-related concerns that individuals had provided to WEC, the types of issues addressed in these concerns, and how WEC's staff addressed these concerns *(p. 100)*.

Election Recount Costs *(p. 101)*

If the Legislature wanted to limit the types of recount costs charged to petitioning candidates, it could modify statutes to require that only certain types of costs could be charged. For example, it could stipulate that petitioning candidates not be charged costs associated with facilities, certain types of equipment, or the salaries and fringe benefits of government employees, who may be expected to fulfill at no cost all duties pertaining to administering elections. Similarly, it could stipulate that recounts must occur in government facilities whenever possible, or require counties to show that they rented reasonably priced private facilities. However, circumstances

such as a public health emergency could result in counties incurring new and unanticipated types of costs, and taxpayer funds could end up financing a portion of the recount costs that petitioning candidates currently cover *(p. 110)*.

If the Legislature wanted to limit the total recount costs charged to petitioning candidates, it could modify statutes to determine the total amount that could be charged. For example, statutes could stipulate an amount per ballot to be recounted, and statutes could stipulate that this amount would increase over time, such as by the rate of inflation. Doing so would ensure a petitioning candidate knew in advance the cost of a recount. However, actual costs could vary considerably among counties, and taxpayer funds could end up financing a portion of the recount costs that petitioning candidates currently cover, particularly if costs increase during circumstances such as a public health emergency *(p. 110)*.

Appendix 9

Statutory Provisions Related to Drop Boxes in Other States[1]

State	Summary of Selected Statutory Provisions
California	Individuals may return absentee ballots to drop boxes that are secure receptacles established by election officials.
Colorado	Individuals may deposit their mail-in ballots in any drop box designated by a county clerk and recorder. A county clerk and recorder must provide at least one drop box per 30,000 registered electors in a county. Drop boxes must be located to provide the greatest convenience to electors.
Georgia	A county Board of Registrars or absentee ballot clerk must establish at least one drop box. A drop box must prevent ballots from being tampered with or removed, be designed to minimize the ability for liquid to be poured into them, and must be labeled "Official Absentee Ballot Drop Box." Such drop boxes are required to be emptied daily.
Hawaii	Clerks may designate securely maintained places of deposit to which individuals can return ballots during the five business days before an election.
Illinois	Election authorities may maintain one or more collection sites for vote-by-mail ballots. These sites must be secured by locks that can be opened only by election authorities, who must collect ballots at the close of business each day.
Montana	An election administrator may designate places of deposit, other than his or her office, to which individuals may return ballots. These places of deposit must be staffed by at least two election officials at all times.
Nevada	Drop boxes are permitted during emergency declarations passed by the Legislature. A county or city clerk must establish at least one location for a ballot drop box to which individuals could return their ballots. A drop box must be constructed of metal or other rigid material, with the capability of being locked, and placed in an accessible and convenient location.
New Jersey	A county Board of Elections must establish at least 10 drop boxes. A drop box must be monitored by camera surveillance, and its location must meet accessibility requirements.
New Mexico	An individual may deposit an absentee ballot in a secured container made available by a county clerk. A secured container must be monitored by camera surveillance and have signage. A county clerk or full-time deputy clerk must collect ballots at least daily from a secured container.
Oregon	A county clerk may designate ballot drop sites that display signage. Individuals may return their ballots to any drop site. The Secretary of State is required to establish by rule security requirements and dates and times of use for drop sites.
Washington	County auditors must provide a ballot drop box at each voting center and at least one other location. County auditors must establish at least one drop box per 15,000 registered voters and at least one drop box in each city, town, and census-designated place with a post office. Ballots must be removed by at least two individuals. After removal, ballots must be transported in secured containers to a counting center.

[1] According to information provided by NCSL, as of September 2020.

Appendix 10

Number of Indefinitely Confined Individuals Who Voted Without Providing Photo Identification, by County[1]

County	Number
Adams	93
Ashland	120
Barron	168
Bayfield	79
Brown	2,455
Buffalo	49
Burnett	73
Calumet	237
Chippewa	367
Clark	99
Columbia	346
Crawford	74
Dane	3,643
Dodge	577
Door	217
Douglas	488
Dunn	215
Eau Claire	741
Florence	32
Fond du Lac	794
Forest	45
Grant	319
Green	216
Green Lake	113
Iowa	127
Iron	66
Jackson	60
Jefferson	425
Juneau	151
Kenosha	1,627
Kewaunee	149
La Crosse	1,027
Lafayette	76

County	Number
Langlade	81
Lincoln	224
Manitowoc	633
Marathon	1,048
Marinette	326
Marquette	72
Menominee	9
Milwaukee	8,592
Monroe	189
Oconto	200
Oneida	357
Outagamie	1,340
Ozaukee	855
Pepin	25
Pierce	201
Polk	216
Portage	399
Price	76
Racine	1,938
Richland	103
Rock	1,237
Rusk	78
Sauk	466
Sawyer	110
Shawano	221
Sheboygan	961
St. Croix	423
Taylor	66
Trempealeau	101
Vernon	99
Vilas	166
Walworth	929
Washburn	75

County	Number
Washington	1,045
Waukesha	3,793
Waupaca	384
Waushara	129
Winnebago	1,277
Wood	560
Total	**44,272**

[1] According to WEC's data on individuals who voted in the November 2020 General Election and who had not previously voted by methods that required them to provide photo identification or did not have photo identification on file with a municipal clerk.

Appendix 11

Statutory Provisions Related to Permanent Absentee Voting for Individuals with Disabilities in Other States[1]

State	Summary of Selected Statutory Provisions
Alabama	Qualified individuals with permanent disabilities that prevents them from going to the polls may apply and be placed on a list that allows ballots to be automatically mailed to them before each election. An application for this process must be signed and notarized by an individual's primary physician. Individuals are required to apply on an annual basis.
Connecticut	An individual who is permanently disabled is eligible for permanent absentee status, which allows the individual to receive an absentee ballot before each election. An individual must provide a certification from a primary care provider stating that the individual is permanently disabled and unable to appear in person at a polling place. Annually, written notices are required to be sent to individuals with permanent absentee status. If such notices are not returned within 30 days these individuals must be removed from permanent absentee status.
Delaware	An individual who is sick or physically disabled may apply in writing for permanent absentee status. Absentee ballots must be sent before each election to all individuals with this status. This status must be removed if an absentee ballot or other correspondence is mailed to an individual and returned as undeliverable, if the individual dies or is otherwise disqualified, or if written notification of a change in status is provided by the individual.
Kansas	An individual with a permanent disability or illness may apply for permanent advance voting status. If an individual fails to vote in four consecutive general elections a notice may be mailed to inform the individual of removal of such status if the individual does not renew their status within 30 days.
Louisiana	An individual who is physically disabled or unable to vote in person, as well as those older than 65 or in nursing or veterans homes, may apply for the Automatic Absentee Ballot Program. An individual must provide a letter from a physician, current mobility impaired identification, or documentation showing eligibility for disability benefits. Individuals will remain within the program until they request to be removed, or until a mailed absentee ballot is returned to the Registrar of Voters Office as undeliverable.
Mississippi	An individual who is permanently physically disabled may apply to automatically receive absentee ballots before each election. An individual must provide a signed statement from a physician or nurse practitioner asserting that the individual is permanently physically disabled and would have difficulty voting in person.
New York	An individual who claims permanent illness or physical disability may apply to receive absentee ballots for all subsequent elections. The mailing of ballots will continue until the individual's registration is cancelled.
Tennessee	A county election commission must establish a permanent absentee voting register for individuals unable to vote in person due to sickness, hospitalization, or physical disability. To be placed on the register, an individual must file a statement from a physician asserting that the individual is medically unable to vote in person.
West Virginia	An individual who is physically disabled and unable to vote in person may apply to be placed on a special absentee voting list. An individual must provide a statement describing the disability and a second statement signed by a physician who concurs with this description. Individuals may remain on such a list until they request to be removed, they are no longer eligible or registered to vote, an absentee ballot is returned as undeliverable, the individual is no longer disabled, or the individual dies.

[1] According to information provided by NCSL, as of September 2020.

Appendix 12

Clerks Who Indicated Receiving Written Complaints about the November 2020 General Election, By County[1]

County	Clerk
Barron	Barron County
Brown	Ashwaubenon, Village of
	Hobart, Village of
	Howard, Village of
Calumet	Calumet County
Chippewa	Cleveland, Town of
Columbia	Lodi, City of
Dane	Dane County
	Deerfield, Town of
	Madison, City of
	Maple Bluff, Village of
	McFarland, Village of
	Mount Horeb, Village of
	Stoughton, City of
	Sun Prairie, City of
Dodge	Chester, Town of
Door	Door County
	Sevastopol, Town of
Dunn	Sherman, Town of
Eau Claire	Eau Claire, City of
Fond du Lac	Friendship, Town of
Grant	Grant County
Green	Brooklyn, Town of
	Green County
	Spring Grove, Town of
Jefferson	Jefferson County
Juneau	Kingston, Town of
	Lemonweir, Town of
Kenosha	Kenosha, City of
	Kenosha County
	Pleasant Prairie, Village of
	Twin Lakes, Village of
Kewaunee	Algoma, City of
La Crosse	La Crosse, City of

County	Clerk
Manitowoc	Manitowoc, City of
Marathon	Kronenwetter, Village of
Marquette	Mecan, Town of
Milwaukee	Greendale, Village of
	Greenfield, City of
	Milwaukee, City of
	Milwaukee County
	Oak Creek, City of
	Shorewood, Village of
	Wauwatosa, City of
Onconto	Oconto County
Oneida	Woodboro, Town of
Outagamie	Buchanan, Town of
Ozaukee	Ozaukee County
	Port Washington, City of
Pierce	River Falls, City of
Price	Harmony, Town of
	Price County
Racine	Mount Pleasant, Village of
	North Bay, Village of
	Union Grove, Village of
Richland	Marshall, Town of
	Richland County
Rock	Beloit, City of
	Rock County
Sheboygan	Sheboygan County
St. Croix	Warren, Town of
Taylor	Taylor County
Trempealeau	Burnside, Town of
Vernon	Bergen, Town of
Vilas	Vilas County
Walworth	Elkhorn, City of
	Walworth County
Washburn	Spooner, Town of

County	Clerk
Washingon	Jackson, Town of
	Richfield, Village of
	Washington County
	West Bend, City of
Waukesha	New Berlin, City of
	Oconomowoc, City of
Waupaca	Waupaca County
Winnebago	Nekimi, Town of
	Oshkosh, Town of
	Winnebago County

[1] As indicated by clerks who responded to our April 2021 survey.

EXHIBIT 18

Presentation, Sheriff, Racine County, Wisconsin (Oct. 28, 2021)

RACINE COUNTY
SHERIFF'S OFFICE

ELECTION INTEGRITY

Protecting Vulnerable Voters

JUDY INVESTIGATED HER MOTHER'S VOTING HISTORY

- Judy went on MyVote Wisconsin (www.myvote.wi.gov) and discovered her mother, Shirley, voted absentee for the November 3, 2020, election

- Shirley died on October 9, 2020 – Before the election

- According to My Vote Wisconsin, prior to being admitted to the Ridgewood Care Facility, Shirley last voted in 2016

JUDY CONTACTS RIDGEWOOD CARE CENTER

- Executive Director stated that the WEC gave facility staff the authority to help residents fill out their ballots

- Judy asked how Shirley could have voted without any knowledge of current events or the news

- The Executive Director stated the staff would ask the residents who they voted for in the past and following party lines that would be their choice

- Judy asked, “So if she could only recall JFK as President, Democrat would be their choice?”

- The Executive Director answered “Yes”

- Judy asked about Shirley’s broken glasses and impaired vision – how can we know the staff member assisting filled in the ballot correctly

- The Executive Director stated he “hoped” the staff would be honest

ORIGINAL COMPLAINT TO THE WISCONSIN ELECTION COMMISSION - NOVEMBER 24TH, 2020

- Judy filed a sworn affidavit with the Wisconsin Election Commission stating that she believed the Ridgewood Care Facility “took advantage” of her mother’s “diminished mental capacity and filled out ballot(s) in her name.”

- Shirley, Judy's Mother
  - Broken glasses – no interest in reading or keeping up on current events
  - Difficulty recognizing her daughter
  - Could not remember her last meal
  - Would not know what day it is
  - Saw flying objects outside of her room that were not there

Mount Pleasant Village Hall

- They received letters from the Wisconsin Election Commission ("WEC") dated March 12, 2020, June 24, 2020, and September 25, 2020, stating that "Municipalities shall not use the Special Voting Deputy process" and should instead mail the absentee ballots

- No notice was posted at any of the facilities because of COVID-19

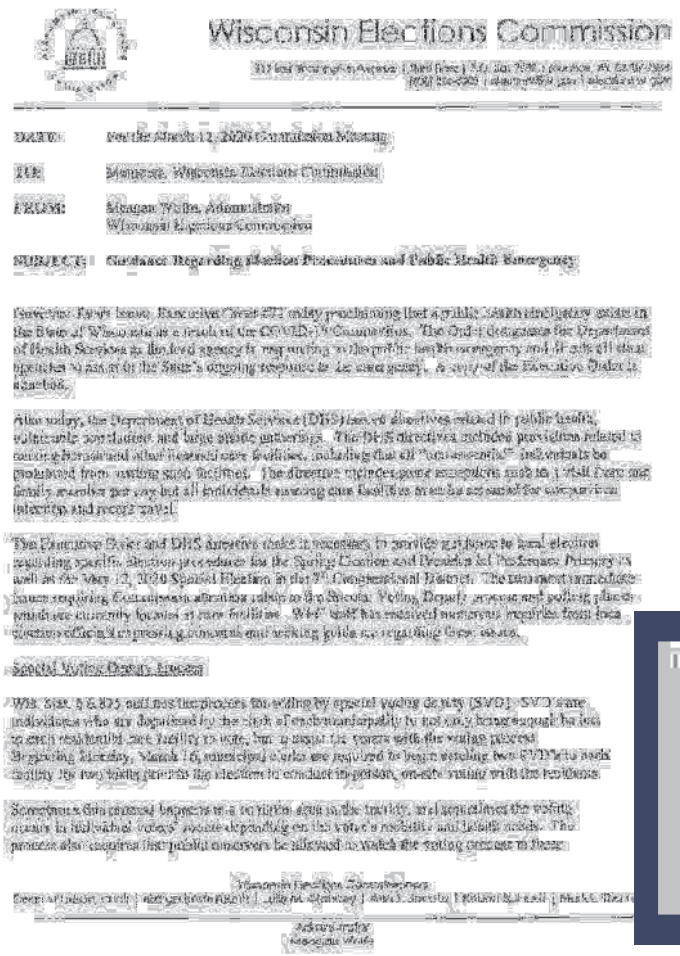
- 42 Ridgewood residents voted

- 38 Ridgewood residents made a fresh request for an absentee ballot during 2020

- The Voting Clerk stated during a Presidential or non-Presidential election, usually approximately 10 people will vote and 0 to 3 people will make a fresh request for an absentee ballot from the Ridgewood Care Center

- RASO received copies of the Request for Absentee Ballots and the Ballot Envelopes

Mount Pleasant Village Hall



Wisconsin Elections Commission

DATE: For the March 12, 2020 Commission Meeting

TO: Members, Wisconsin Elections Commission

FROM: Meagan Wolfe, Administrator
Wisconsin Elections Commission

SUBJECT: Guidance Regarding Election Procedures and Public Health Emergency

Governor Tony Evers issued Executive Order #72 today proclaiming that a public health emergency exists in the State of Wisconsin as a result of the COVID-19 Coronavirus. The Order designates the Department of Health Services as the lead agency in responding to the public health emergency and directs all state agencies to assist in the State's ongoing response to the emergency. A copy of the Executive Order is attached.

Also today, the Department of Health Services (DHS) issued directives related to public health, substantial gatherings and large sports gatherings. The DHS directives includes provisions related to nursing homes and other residential care facilities, including that all "non-essential" individuals be prohibited from entering such facilities. The directive includes some exceptions and to wit, visits may be made by any but all individuals entering care facilities must be screened for symptoms, identity and record travel.

The Executive Order and DHS directive make it necessary to provide guidance to local election officials regarding specific election procedures for the Spring Election and Presidential Preference Primary as well as the May 12, 2020 Special Election in the 7th Congressional District. The immediate issues requiring Commission direction relate to the Special Voting Deputy process and polling places which are currently located at care facilities. WEC staff has received numerous requests from local election officials requesting guidance and seeking guidance regarding these issues.

Special Voting Deputy Process

Wis. Stat. § 6.875 sets out the process for voting by special voting deputy (SVD). SVD's are individuals who are appointed by the clerk of each municipality to not only have equal access to each residential care facility to vote, but to assist the voters with the voting process. Beginning Monday, March 16, municipal clerks are required to begin sending two SVD's to each facility for two days prior to the election to conduct in-person, on-site voting with the residents.

Sometimes this process takes a toll on staff and facility, and sequesters the voting process to individual voters' rooms depending on the voter's mobility and health needs. The process also requires that public observers be allowed to watch the voting process in these

Wisconsin Elections Commission
Dean Knudson, Chair | Mark Gaber, Secretary | Amy Chaney, Treasurer | Bernie Ewen | Marge Bennett

Administrator
Meagan Wolfe

1) In light of Executive Order #72 and directives of the Department of Health Services, the Commission finds that Special Voting Deputies are "non-essential" individuals who are not permitted to enter nursing homes and other care facilities without completing a screening process that is not feasible to implement prior to the Spring Election and Presidential Primary. For that election and the May 12, 2020 Special Election in the 7th Congressional District, the Commission directs that municipalities shall not use the Special Voting Deputy process to serve residents in care facilities and instead shall transmit absentee ballots to those voters by mail.

SOURCE: WISCONSIN ELECTIONS COMMISSION LETTER - MARCH 12, 2020

Review of Documents

APPLICATION FOR ABSENTEE BALLOTS

- Pre-filled out by facility staff

- The Certification of being “indefinitely confined” pre-checked by staff

OR

- The Certification of being “indefinitely confined” post-checked by the municipal clerk

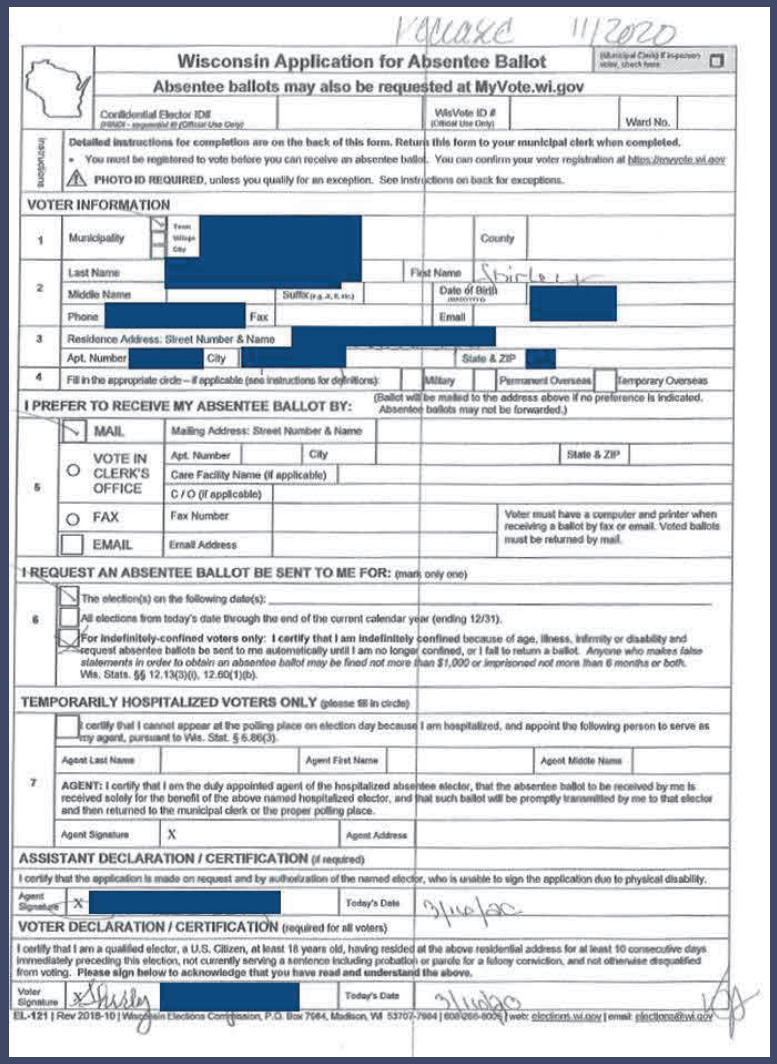
VOTER ENVELOPES

- Certification of Witness – Facility staff

WEC LETTERS TO MUNICIPAL CLERKS

- Coordinate with the dates of the open meetings by the WEC
- Open meetings can be viewed on WisEye www.wiseye.org

Review of Documents



Wisconsin Application for Absentee Ballot

Absentee ballots may also be requested at MyVote.wi.gov

Confidential Elector ID# | WisVote ID # | Ward No.

Detailed instructions for completion are on the back of this form. Return this form to your municipal clerk when completed.

- You must be registered to vote before you can receive an absentee ballot. You can confirm your voter registration at https://myvote.wi.gov

PHOTO ID REQUIRED, unless you qualify for an exception. See instructions on back for exceptions.

VOTER INFORMATION

1 Municipality | County

2 Last Name | First Name | Middle Name | Suffix | Date of Birth | Phone | Fax | Email

3 Residence Address: Street Number & Name | Apt. Number | City | State & ZIP

4 Fill in the appropriate circle – if applicable (see instructions for definitions): Military | Permanent Overseas | Temporary Overseas

I PREFER TO RECEIVE MY ABSENTEE BALLOT BY: (Ballot will be mailed to the address above if no preference is indicated. Absentee ballots may not be forwarded.)

5 MAIL | Mailing Address: Street Number & Name

VOTE IN CLERK'S OFFICE | Apt. Number | City | State & ZIP | Care Facility Name (if applicable) | C / O (if applicable)

FAX | Fax Number | Voter must have a computer and printer when receiving a ballot by fax or email. Voted ballots must be returned by mail.

EMAIL | Email Address

I REQUEST AN ABSENTEE BALLOT BE SENT TO ME FOR: (mark only one)

6 The election(s) on the following date(s): _____

All elections from today's date through the end of the current calendar year (ending 12/31).

For indefinitely-confined voters only: I certify that I am indefinitely confined because of age, illness, infirmity or disability and request absentee ballots be sent to me automatically until I am no longer confined, or I fail to return a ballot. *Anyone who makes false statements in order to obtain an absentee ballot may be fined not more than $1,000 or imprisoned not more than 6 months or both.* Wis. Stats. §§ 12.13(3)(i), 12.60(1)(b).

TEMPORARILY HOSPITALIZED VOTERS ONLY (please fill in circle)

7 I certify that I cannot appear at the polling place on election day because I am hospitalized, and appoint the following person to serve as my agent, pursuant to Wis. Stat. § 6.86(3).

Agent Last Name | Agent First Name | Agent Middle Name

AGENT: I certify that I am the duly appointed agent of the hospitalized absentee elector, that the absentee ballot to be received by me is received solely for the benefit of the above named hospitalized elector, and that such ballot will be promptly transmitted by me to that elector and then returned to the municipal clerk or the proper polling place.

Agent Signature | X | Agent Address

ASSISTANT DECLARATION / CERTIFICATION (if required)

I certify that the application is made on request and by authorization of the named elector, who is unable to sign the application due to physical disability.

Agent Signature | X | Today's Date

VOTER DECLARATION / CERTIFICATION (required for all voters)

I certify that I am a qualified elector, a U.S. Citizen, at least 18 years old, having resided at the above residential address for at least 10 consecutive days immediately preceding this election, not currently serving a sentence including probation or parole for a felony conviction, and not otherwise disqualified from voting. Please sign below to acknowledge that you have read and understand the above.

Voter Signature | X | Today's Date

EL-121 | Rev 2018-10 | Wisconsin Elections Commission, P.O. Box 7984, Madison, WI 53707-7984 | 608/266-8005 | web: elections.wi.gov | email: elections@wi.gov

SOURCE: WISCONSIN APPLICATION FOR ABSENTEE BALLOT - MARCH 16, 2020

6.84 WISCONSIN STATUTE

LEGISLATIVE POLICY. The legislature finds that voting is a constitutional right, the vigorous exercise of which should be strongly encouraged. In contrast, voting by absentee ballot is a privilege exercised wholly outside the traditional safeguards of the polling place. The legislature finds that the privilege of voting by absentee ballot must be carefully regulated to prevent the potential for **fraud or abuse**; to prevent **overzealous solicitation** of absent electors who may prefer not to participate in an election; to prevent **undue influence** on an absent elector to vote for or against a candidate or to cast a particular vote in a referendum; or other similar abuses.

6.875 WISCONSIN STATUTE

Absentee Voting in Facilities

- This statute is the **"exclusive means"** of absentee voting in residential care facilities
- **Shall** dispatch two Special Voting Deputies ("SVDs") to the facility
- The SVDs **shall** personally deliver the ballot
- **NO employee (or past employee of the last two years) may be an SVD**
- Notice of the SVDs visit **shall** be posted at the facility
- The SVDs **shall** witness the vote and **may assist** in marking the ballot
- The SVDs **shall NOT** accept an absentee ballot not issued by an SVD
- **No individual** other the a SVD or relative **may assist** the voter
- The SVDs **shall** seal the ballot envelope and deliver it to the clerk

6.875 WISCONSIN STATUTE

Absentee Voting in Facilities

•§ 6.875(6)(e) – "If a qualified elector is not able to cast his or her ballot on 2 separate visits by the deputies to the home or facility, the deputies shall so inform the municipal clerk . . . Who may then send the ballot to the elector . . ."

The WEC falsely reasoned that since the Special Voting Deputies could not be allowed into any facilities, the Special Voting Deputies "program" could be "suspended", and the municipalities could go directly to the mailing process. The WEC also improperly/illegally advised the facilities to have staff members assist the residents in voting.

UNITED STATES CONSTITUTION

Article II, Section 1, paragraph 2 – The state legislature is to determine the “Manner” in which the President is elected

Article I, Section 4, paragraph 1 – It is up to the state legislature to determine “the Times, Places and Manner of holding Elections for Senators and Representatives”

RIDGEWOOD CARE FACILITY
DECEMBER 18, 2020

- The Executive Director stated he “hoped” his staff was “honest” while marking the voting ballot for the residents

- The Director of Recreational Therapy stated that if a resident could only point to the ballot, her staff would fill in the appropriate dot

- The Director of Recreational Therapy was “confident” Shirley wanted to vote, but then admitted she did not have contact with Shirley – her staff would have contact with the residents

- The Activities Aid stated if the resident did not want to vote, she would come back later
  - The Activities Aid stated she would leave the news channel on for a few days and then come back and see if the resident wanted to vote (List of preferred channels or NBC)
  - The Activities Aid stated she would keep the ballots in her desk drawer when she was waiting for the residents to decide to vote

RIDGEWOOD CARE FACILITY
DECEMBER 18, 2020

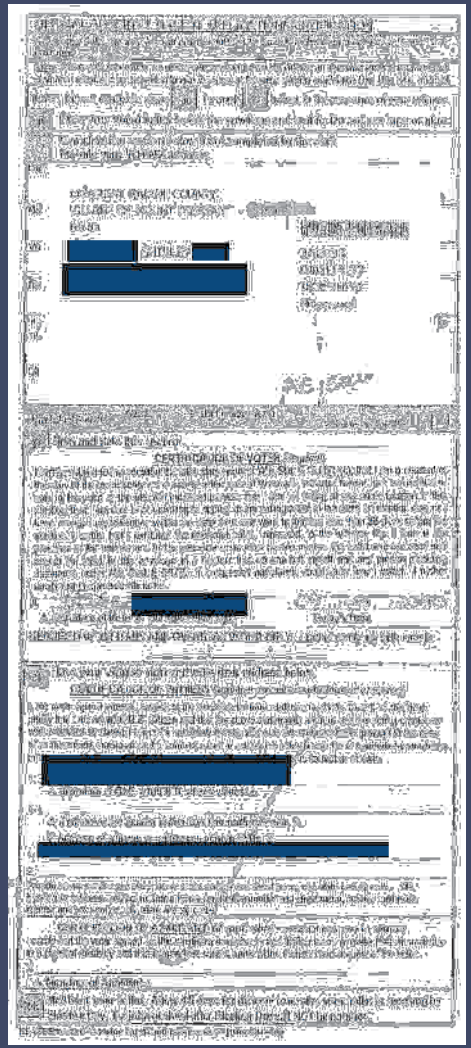
- The procedure implemented by the facility did not comply with the instructions on the ballot envelope

- The Director of Recreational Therapy and the Activities Aids agreed that:

  - If the resident did or did not vote, the Activities Aid would place the ballot in the envelope (unsealed) and give it to the Director of Recreational Therapy

  - The Director of Recreational Therapy would seal the ballot envelope and mail it to the municipal clerk

Review of Documents



SOURCE: WISCONSIN APPLICATION FOR ABSENTEE BALLOT ENVELOPE - SEPTEMBER 22, 2020

Other Concerned Families

DF was adamant that her mother, OF, would not have requested an absentee ballot. She was unable to remember what she ate for breakfast that day. DF stated, “It is so hard to get her to sign something, even things that I need, you know, to conduct business, it is very hard to get her to sign anything. So, she would not have requested a ballot and then sat there and signed it, no. I just don’t believe that.” **According to My Vote Wisconsin (Since 2012), there is no record of OF voting in any other election.**

RP stated that her father, NG, had difficulty recognizing his own grandchildren. He would not know that Trump was the president nor who was elected the new president, and he would not know what the candidates stood for on the issues. RP stated NG only asked about “Doritos” and “Snickers”. According to My Vote Wisconsin (Since 2012), there is no record of NG voting in any other election. When asked if NG would have the mental ability to express his desire for an absentee ballot and exercise his right to vote, RP responded, “No! No, I’m sorry, no!”. **According to My Vote Wisconsin (Since 2012), there is no record of RP voting in any other election.**

Other Concerned Families

LM stated her mother, RL, is confused, not sure where she is, does not recognize her own children, and is not right in her own mind. LM stated RL would not have known who the candidates were, and someone had to have taken advantage of her. **According to MyVote Wisconsin (since 2012), there is no record of RL voting in any other election.**

RS stated his mother, FP, is 102-years-old and is experiencing dementia. RS stated that FP is starting to forget to eat; that she cannot recognize her own children; that she is starting to forget to eat; and that she only remembers the past. **According to MyVote Wisconsin (since 2012), FP voted in this election and an election in 2012.**

TM stated his father, MR, did not have the desire to vote absentee. TM stated MR informed her and her mother that if he cannot vote in person, he did not want to vote. **According to MyVote Wisconsin (since 2012), there is no record of MR voting in any other election.**

Other Concerned Families

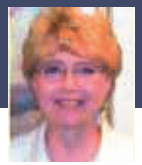
RM is the legal guardian for SL, and RM stated that SL has been determined to be incompetent by a probate court. RM stated she believed SL's right to vote had been taken away. RM stated SL is unable to make any decisions for herself and she has no ability to know what is going on. RM stated SL would not know how to request an absentee ballot. RM stated SL is not allowed to sign any legal documents because she is so impaired. RM stated SL would have no inclination to vote and she would have no idea what she was doing. AS stated, her mother, SL, was suffering from dementia and she did not have the sound mind necessary to request an absentee ballot and to exercise her right to vote. **According to MyVote Wisconsin (since 2012), SL voted in this election and an election in 2012**

GH stated his mother, BH, would ask him, "Who are you?" and GH would respond, "I'm your youngest boy." GH stated BH believed her own mother died a few weeks ago but her mother actually died in 1965. **According to My Vote Wisconsin (since 2012), BH voted in two elections in 2020 and no other elections.**

WISCONSIN ELECTIONS COMMISSION

SECRETARY

Marge Bostelmann



COMMISSIONER

Julie M. Glancey

CHAIR

Ann S. Jacobs

COMMISSIONER

Dean Knudson

COMMISSIONER

Robert F. Spindell, Jr.

VICE-CHAIR

Mark L. Thomsen

WISCONSIN ELECTIONS COMMISSION -
HTTPS://ELECTIONS.WI.GOV/INDEX.PHP/ABOUT/MEMBERS

Timeline

MARCH 10, 2020

- The WEC sent a letter to the Governor requesting the "suspension" of "several provisions of Wisconsin election law"
    - Special Voting Deputies
    - Moving the location of polling places

- The Governor's Office informed the WEC that **the Governor does not have the power to "suspend" parts of Wisconsin's voting law during an emergency**

MARCH 12, 2020

- Governor Ever's issued Executive Order #72

- The WEC issued a directive stating Special Voting Deputies shall not be sent to facilities

- Commissioner Knudsen, "what we are really saying here, is once again, we are saying that, despite what the law says, the election commission is saying, in this instance, we need to have some flexibility, **to not follow the law."**

Timeline

MAY 26, 2020

- Governor's extended "Safer at Home" order expires

JUNE 24, 2020

- The WEC extended their previous March 12, 2020, orders

- Commissioner Knudson, **"We need to go back to following the law**, but for the Special Voting Deputies, following the letter of the law here would mean putting hundreds and hundreds of nursing home residents' lives at severe risk. There is got to be a way to do this without doing that."

- Commissioner Spindell was concerned **with fraud in nursing homes** and suggests PPE's

Timeline

SEPTEMBER 16, 2020

- The WEC extended their previous March 12, 2020 orders

- Commissioner Spindell stated the law stated the WEC is supposed to do something, and the WEC is not doing that task – **Spindell asked where that power came from. He also suggested use of technology to facilitate Special Voting Deputies.**

- Commissioner Knudson stated, "My thinking going back to March on this, from the time I first communicated with the Governor saying I thought that **we should not follow this law during this pandemic**."

- Chair Jacobs stated the "state law" or "rulings of DHS" would not allow for Special Voting Deputies inside of facilities

Review of Documents

How to assist the voter in filling out their absentee ballot

If a voter requests assistance, you may read the ballot, including candidate names, party affiliations and ballot instructions, to the voter or mark the ballot as directed by the voter. If the voter asks questions about individual candidates or their political platform, you cannot answer those questions. You cannot in any way prompt the voter to vote for a particular candidate. If uncertain for whom to vote, the voter may decide to leave a contest unvoted. After assisting the voter, you will sign the ballot in the box that says, "Certification of Voter Assistance."

Absentee Voting at Care Facilities in 2020

Your Role as a Care Facility Administrator

In a typical election, Special Voting Deputies (SVDs) may be coming into your facilities and conducting absentee voting with your residents. However, due to safety concerns, SVDs will not be entering your facility for the November election. Instead ballots will be mailed out to individual voters with current requests on file. Many care facility and nursing home residents rely on family members for assistance in voting. Because most care facilities and nursing homes are not allowing guests at this time, some voters may require assistance from care facility staff to vote. We know that this may be difficult for many facilities due to competing priorities and staffing. This document will provide resources to make absentee voting and registering to vote as smooth as possible for your facility and your residents.

As a care facility administrator or staff member, you are able to:

- Assist residents in filling out their ballots or certificate envelopes.
- Assist residents in completing voter registration forms and absentee requests.
- Sign the special certificate envelope (EL-122sp) if necessary (see below for explanation).
- Witness ballots.

Absentee Voting for Residents of Your Facility

Ballots began being mailed out on September 17 for voters with current absentee requests on file for the November 3 election. Most ballots will be mailed to voters, but some clerks have indicated that they are hand delivering ballots to care facilities in a large envelope or other sealed container. After receiving ballots, you must distribute ballots individually to those voters. If a voter no longer lives in your facility or is deceased, please mark the ballot carrier envelope "moved" or "deceased" and return it to the municipal clerk as soon as possible.

Each absentee carrier envelope should contain the ballot, an instruction sheet and a certificate envelope used to return the ballot (referred to as the EL-122).

How to assist the voter in filling out their absentee ballot

If a voter requests assistance, you may read the ballot, including candidate names, party affiliations and ballot instructions, to the voter or mark the ballot as directed by the voter. If the voter asks questions about individual candidates or their political platform, you cannot answer those questions. You cannot in any way prompt the voter to vote for a particular candidate. If uncertain for whom to vote, the voter may decide to leave a contest unvoted. After assisting the voter, you will sign the ballot in the box that says, "Certification of Voter Assistance."

Wisconsin Elections Commission
212 East Washington Avenue | Third Floor | P.O. Box 7984 | Madison, WI 53707-7984
(608) 266-8005 | elections@wi.gov | elections.wi.gov

SOURCE: ABSENTEE VOTING AT CARE FACILITIES IN 2020 - SEPTEMBER 25, 2020

Timeline

JANUARY 15, 2021

- The WEC extended their previous March 12, 2020, orders
- Commissioner Knudson:
  - Expressed his concern that the "policy" of the WEC was **"telling the clerks to break the law"** and he stated, "But I continue to have great discomfort with the idea that our motion is going to direct them, **that we're the ones directing them to break the law.**"
  - Suggested **the use of technology so that all of the policies "as required by law are being followed".**
  - The **"SVD law is a law"** and "some of the **prohibitions on visitors at nursing homes . . . was a guidance, a directive."**

Timeline

FEBRUARY 11, 2021

- Legislative Council provided an opinion to the Joint Committee for the Review of Administrative Rules (JCRAR) that **state law does not empower the WEC to waive the Special Voting Deputies, nor does the law contain an exemption for a pandemic**

- **JCRAR notified the WEC to promulgate an emergency rule or cease issuing such directives**

MARCH 2, 2021

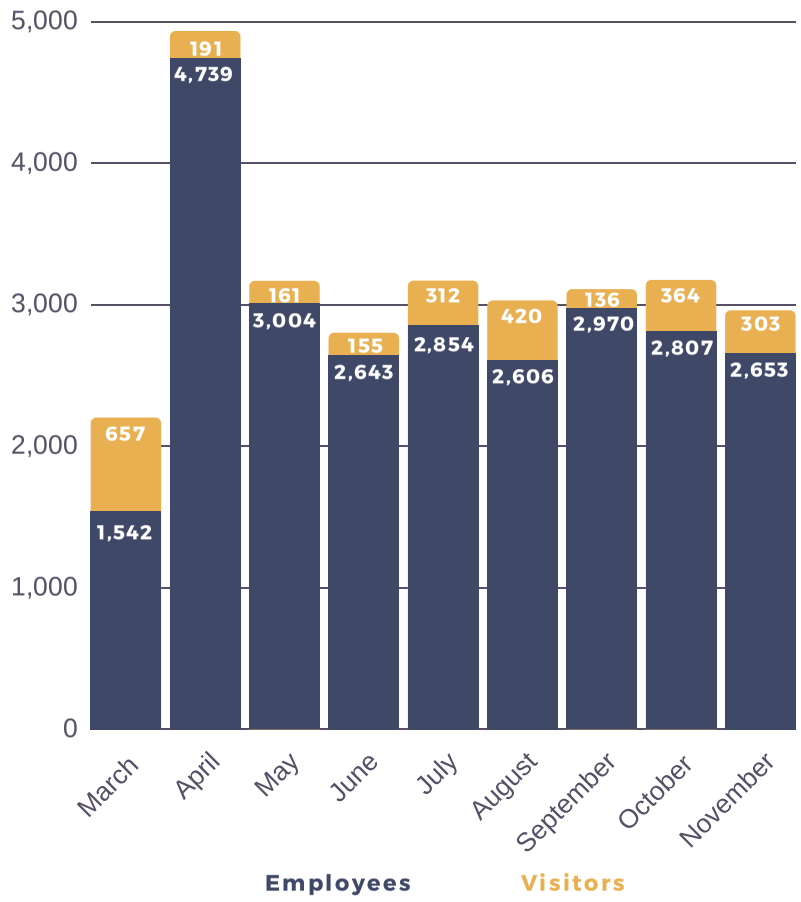
- WEC amends their directive and now calls for Special Voting Deputies to be sent to facilities two times prior to mailing the ballot

Ridgewood Care Facility

Employees and Visitors

333 Employees

899 Visitors



TYPES OF VISITORS

Interview or Job Interview

24 Times

Instructor

4 Times and 19 Times with Students

Orkin Service

19 Times

Vendor/Vending Machine

17 Times

Kitchen or Kitchen Repair

17 Times

Cleaning Fish Tank, Cleaning Tanks, or Tank Maintenance

11 Times

Elevator

10 Times

Laundry or Laundry Repair

8 Times

TYPES OF VISITORS

Maintenance

6 Times

Copier

4 Times

Clean Bird Cage

3 times

Inspection

2 times

Looking for a Job

DoorDash Delivery

12.13 WISCONSIN STATUTE

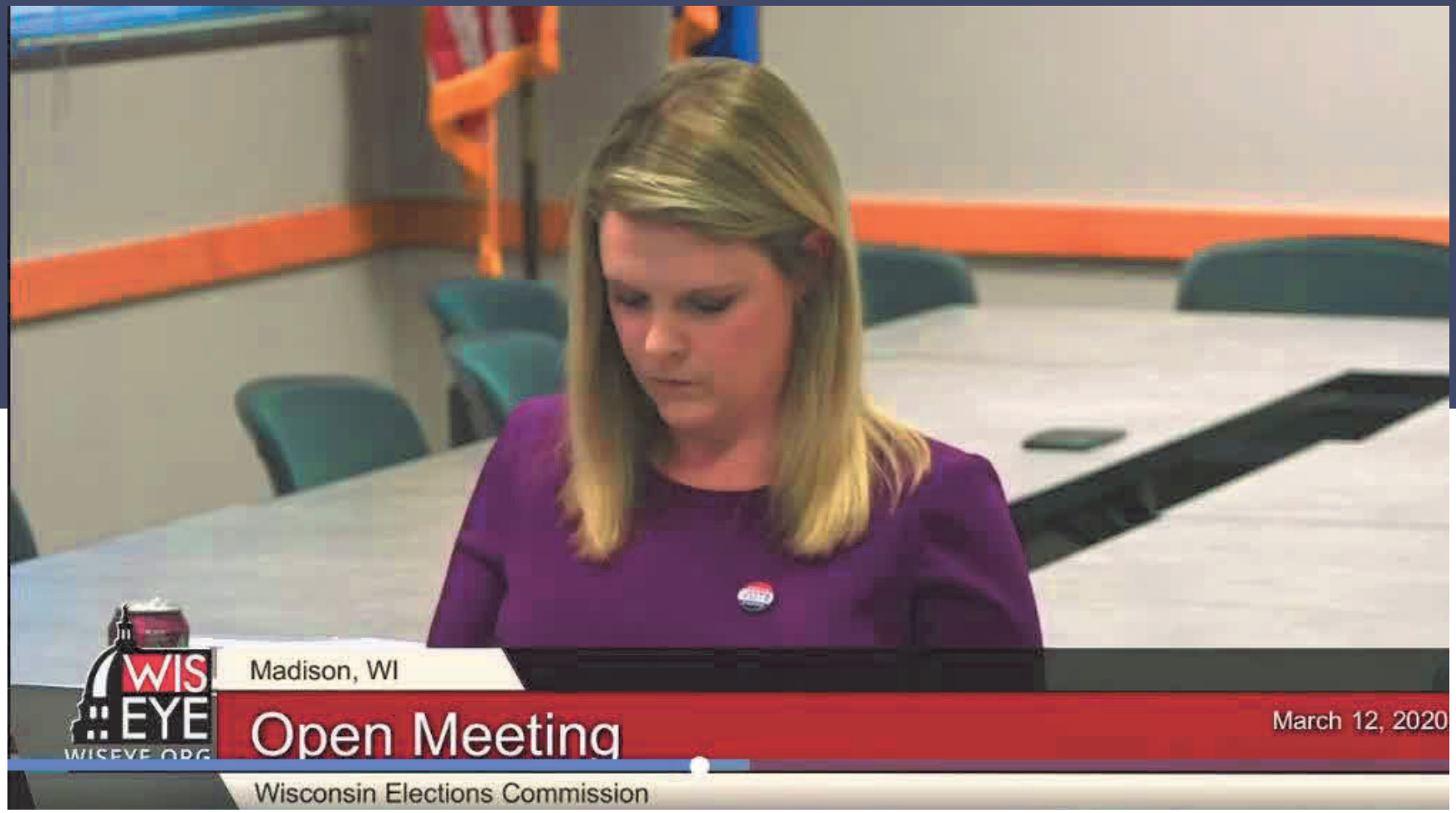
Election Fraud

- § 12.13(2)(b)(7) – "In the course of the person's official duties or on account of the person's official position, intentionally violate or intentionally cause any other person to violate any provision of chs. 5 to 12 for which no other penalty is expressly prescribed."

- § 12.13(3)(n) – "Receive a ballot from or give a ballot to a person other than the election official in charge."

- § 12.13(3)(p) – "Receive a completed ballot from a voter unless qualified to do so."

- § 12.13(3)(s) – "Solicit another elector to offer assistance under s. 6.82 (2) or 6.87 (5), except in the case of an elector who is blind or visually impaired to the extent that the elector cannot read a ballot."


WIS EYE
WISEYE.ORG
Madison, WI
Open Meeting
March 12, 2020
Wisconsin Elections Commission

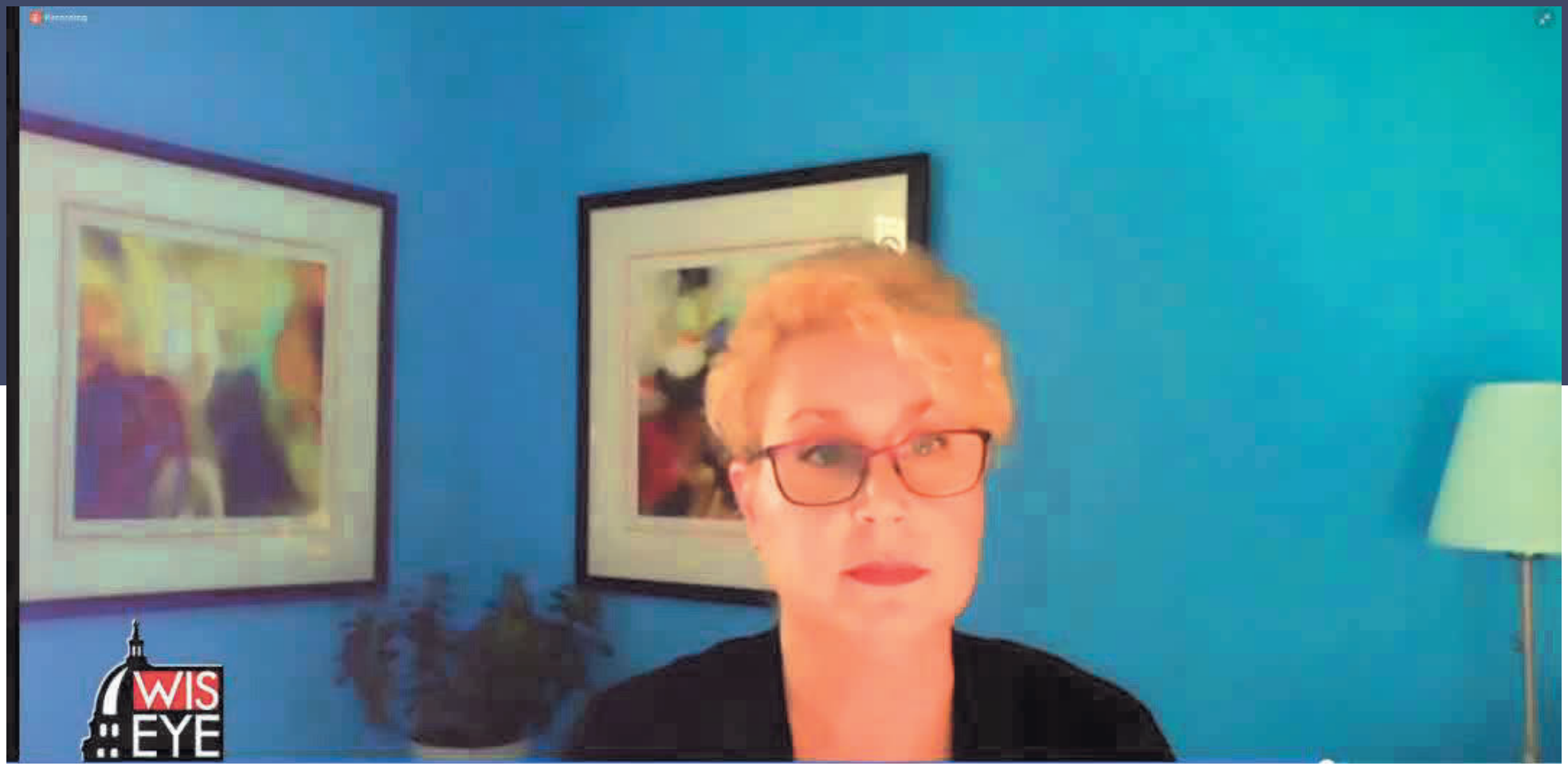
What are you looking for?

Wisconsin Elections Commission Special Teleconference Meeting

On June 24, 2020, the Wisconsin Elections Commission held a **special teleconference meeting** to discuss Special Voting Deputies for the August Election.

Categories: Meetings

WIS EYE
@WI_Elections
Wisconsin Elections Commission
September 16, 2020


WIS
EYE

WIS EYE
@WI_Elections
Wisconsin Elections Commission Meeting
Robert F. Spindell, Jr
Septemebr 16, 2020

WIS EYE
WISEYE.ORG
@WI_Elections
Wisconsin Elections Commission
January 15, 2021
12:45 PM
Special Teleconference Meeting

WIS EYE
WISEYE.ORG
@WI_Elections
Dean Knudson
January 15, 2021
1:24 PM
Commissioner - Wisconsin Elections Commission

Moving Forward

Wisconsin State Legislature

Wisconsin State Legislature

Governor

Tony Evers
Office of the Governor | State of Wisconsin

Attorney General

Wisconsin Department of Justice
Office of the Attorney General

Wisconsin Elections Commission

262-636-3853

voterintegrity@racinecounty.com

EXHIBIT 19

First Interim Rept., Wisconsin Office of the Special Counsel (Nov. 10, 2021)

Office of the Special Counsel

First Interim Report

Delivered to the Wisconsin State Assembly November 10, 2021

"I am writing this, as I feel my mother was taken advantage of in her mental state. Parents and loved ones should be protected, not exploited, for an ink mark on a piece of paper and questionable agenda." *Judy Weshphal-Mitchell, discussing how actions of the Wisconsin Election Commission affected her family*

Elections in the United States are the bedrock of our constitutional republic. They are subject to the law, including the fundamental laws found in the Constitutions of the United States and the State of Wisconsin. But fair elections are not a mere checkbox exercise. To secure republican government it is important not just that the law is followed, but that the citizens have confidence the law is followed. In the run up to the election of November 3, 2020, polling showed a majority of Americans did not have confidence their vote would count. In a democracy, this is as untenable as it is unacceptable.

To help address these concerns, the state Assembly established a new office, the Office of the Special Counsel, to investigate the recent elections in our state. As head of this new office, I am authorized by law to take all reasonable steps to investigate what happened in regard to the November 2020 election, what should have happened, why there was a difference between the two, and to recommend steps to enhance the transparency of our elections as well as restore public confidence in elections going forward.

This interim report is a first step in discharging that mission.

While this report does not definitively answer all questions that might be asked about the November 2020 election, it takes an important step in collating those questions and presenting them in a structured manner.

Over the approximately sixty days since my office was created and has been funded, we have spoken with, and listened to, everyone who has wanted to talk. This open-door policy will remain throughout the entirety of this investigation, and any future investigation with which this office is charged. We have drawn some criticism from those in the media who would suggest my discussions with various individuals or groups implies an endorsement of their views. This is not the case. I do not apologize for this open-door policy: the views of all Wisconsinites matter and sidelining or even laughing

at serious concerns of any citizen of this state would call into question whatever may be discovered by my investigation.

In the short time the Office of the Special Counsel has been funded, we have not only met with many individuals and groups, but we have collected, and in some cases compelled by law, the production of relevant information. Further, our investigation has gone beyond, and will continue to go beyond, the investigation recently conducted by the Legislative Audit Bureau (LAB). One purpose of this interim report is to lay out for the public how my Office's investigation differs significantly from the LAB investigation.

Notwithstanding lawsuits and threats of more lawsuits supported by high-priced, out-of-state lawyers, my office expects to depose government officials, under oath, to determine whether state and federal law were followed in our elections, whether good management held, and if not, who might have been responsible. If necessary, we stand prepared to refer all relevant information to appropriate state and federal law enforcement authorities. The wagon-circling by government entities in our state is concerning and is not limited to my investigation: the City of Madison, the City of Milwaukee, and the town of Little Suamico all refused to fully cooperate even with the LAB investigation, cooperation to which our legislature and the people are entitled by our State Constitution.

Make no mistake: I sincerely hope the law was followed in Wisconsin. It would give me the greatest satisfaction to deliver to the speaker of the Assembly and the public a final report which analyzes the November 2020 election in a complete and thorough manner, concludes no major overhaul of our laws or practice are necessary, and the election was administered in a legal and appropriate manner. And yet, as the following interim report demonstrates, many important questions remain unanswered. These questions include: were all lawful votes, and only lawful votes, counted? Did the machines work as advertised and expected? Were all election processes followed to the letter? Did clerks and other election officials have all the tools they needed to deal with the unprecedented

challenge posed by the COVID lockdowns and historic levels of absentee voting? Did outside corporate money unduly influence the election and/or the administration of the election? Above all, what changes can the state of Wisconsin make to ensure our future elections are not only secure, but as important, widely known to be secure?

In the coming weeks, my Office will continue to collect and analyze information about the November 2020 election, because the public has a right to know what happened. I have no partisan agenda: I am not running for office, and I do not know of any lawful remedy in the state of Wisconsin to change the certification of its electors from our current President Joe Biden to former President Donald Trump. Furthermore, I do not come with preconceived answers to any questions. Why were so many voter registrations at a single address? Why were so many voter registrations given under a single phone number? Why was there a "blip" at 4:00 a.m. in the reported statewide returns the morning after the election? All of these questions may have innocent explanations. My investigation intends to discover facts which will allow the legislature and the people of Wisconsin to draw their own conclusions about the integrity of the November 2020 election.

Many of these answers might have already been obtained were it not for unjustified obstruction of this investigation. Specifically, I requested information from the Wisconsin Elections Commission (WEC) and certain clerks about election procedures and information they possessed. With a large degree of political theater, some of this information has been withheld. I issued subpoenas, as I am lawfully authorized to do as part of my Office's investigation as a function of legislative oversight. Rather than simply provide the information, WEC has filed a lawsuit in an attempt to quash the subpoenas and avoid providing governmental data and information to my office. I am aggressively defending the subpoenas in our state courts—courts which I once helped to oversee in my capacity as a Justice—but WEC's actions beg the question: What are WEC and the recalcitrant city clerks hiding from the public and our legislature?

Nevertheless, I have had many productive conversations with government officials. In fact, in the many discussions my Office has had with the fine public servants in the state of Wisconsin, I have learned that complicated questions may have simple answers. But many complicated questions deserve honest answers that take time to process and report. I ask each reader of this interim report to take this as a jumping-off point for learning about the administration of elections in Wisconsin. And again, please reach out to my office if you have any information of relevance. Your voice matters.

Michael J. Gableman

Special Counsel

What is the OSC Investigation?

November 3, 2020, was election day nationwide, and was, in our State of Wisconsin, the culmination of months of work by dedicated election workers and volunteers. It was a monumental and expensive undertaking which is critical to our representative democracy. However, it is beyond debate that questions remain about the integrity of that election. In discharging its duty under both the Federal and State Constitutions, the Wisconsin State Assembly saw fit, on June 26, 2021, to appoint a Special Counsel, establish the Office of the Special Counsel to investigate the election, make findings, and report those findings and recommendations to the Assembly. This report is a first step in fulfilling that duty.

The Office of the Special Counsel is an authorized agency of the State of Wisconsin. Its staff, including and especially the Special Counsel himself, take care to abide by all applicable state and federal laws, including open records laws and regulations relating to the practice of law. My Office will abide by the highest ethical standards to maintain a commitment to transparency, inclusion, and accountability. As such, the Office has established various internal policies, continues to maintain records, and commits to full disclosure of all public records upon the conclusion of the present investigation.

To-date, my Office has already collected and reviewed thousands of governmental and other documents. My Office has interviewed numerous witnesses and will continue to do so until the conclusion of the present investigation. The Office has been allocated a comparatively modest budget and has relied heavily upon volunteers and input by citizens' groups: the vast majority of the Office's budget, while allocated, has not been spent.

The Office may be reached at (262) 202-8722 or online at www.wifraud.com. As noted below, testimony compelled by this Office bears with it the promise, mandated by Wisconsin law, that any information so compelled may not be used in a criminal

proceeding against the individual from whom it was provided. *See* Wis. Stat. § 13.35. This Office has already been in contact with certain whistleblowers and commits to taking all steps to protect their interests and those of future whistleblowers.

Constitutional Authority

Pursuant to the federal Constitution, Article I, Section 4, it is state legislatures who are authorized to set "The Times, Places and Manner of holding Elections for Senators and Representatives…" The Supreme Court of the United States has clarified that this means the Wisconsin legislature bears primary responsibility for establishing rules regarding things like voter registration, poll watching, penalties, ballot counting, and certification. This primacy of the state legislature is ratified by the Wisconsin Constitution, which in Article IV, Section 1 declares "The legislative power shall be vested in a senate and assembly." Whether this means the state Assembly and Senate may, by joint resolution and without gubernatorial signature, tighten up or loosen election security for federal elections, and whether there are limits on how much of this constitutional responsibility can and should be delegated to other state actors (such as the Wisconsin Elections Commission), is an open question in state law.

There is some debate that the Elections Clause of the United States Constitution authorizes states to regulate legislatures alone to dictate the time, places, and manner of elections. While the word "legislature," is used several times in the federal constitution, its meaning differs according to the context in which it appears, dependent upon the character of the function which the legislature is called upon in each respective instance to exercise. *Ariz. State Legislature v. Ariz. Indep. Redistricting Comm'n*, 576 U.S. 787, 808 (2015) (citing *Atlantic Cleaners & Dyers, Inc. v. United States,* 286 U.S. 427, 434 (1932)). Even if the constitution authorizes the Assembly and Senate to jointly amend parts of our election code without gubernatorial signature, the Wisconsin constitution provides that the legislature should create bills of law which become effective only when signed by the governor. Wis. Const. Art. 4, Section 17; Article 5, Section 10. It may be the case that the

Senate and Assembly can change election regulations in the absence of a statute on the books, indeed Wisconsin law appears silent on this question, but it would be another matter for the Senate and Assembly to seek to repeal an extant portion of the election code.

This brings up a second, equally important issue—certification of the vote. There are serious and legitimate questions that the certification of Wisconsin's election results may have been undertaken in an unlawful and unconstitutional manner. While the Wisconsin legislature has specified how presidential electors are selected, that statute does not empower the governor or WEC to certify the results of the election. The acceptance of electors by the governor while recount challenges were pending deprived the legislature of the right to certify the vote pursuant to Article II of the United States Constitution. Hasty certification of electors in a tightly contested election may disenfranchise voters to the same extent as missing a deadline and failing to certify electors at all. While hasty certification may violate the state constitutional duties of the legislature, delaying certification of electors until resolution of relevant issues does no such violence to our legal system.

Statutory Authority

The authority of the Legislature brings with it the legislative prerogative to gather information, debate bills, and pass laws. In discharging these duties, the legislature bears the constitutional obligation and has the authority to conduct oversight, including the ability to compel production of documents and testimony. Under Wis. Stat. § 13.31, the legislature has the authority to subpoena information from individuals. Because this legislative subpoena is a part of common law legislative authority which holds that without access to all available information a legislature cannot properly legislate—and because this subpoena does not directly relate to or contemplate criminal proceedings, criminal due process rights are not implicated. *See* Wis. Stat. § 13.35. To this end, § 13.35 expressly provides that documents and testimony provided by a witness pursuant to a

legislative subpoena cannot "be used in any trial or criminal proceeding against such person in court." This does not preclude this Office from turning over information to relevant law enforcement agencies, or by talking with this Office any given individual is somehow immune from criminal prosecution.

This office has, to-date, issued seventeen subpoenas for documents as well as testimony for governmental information from sitting government officials and has obtained some voluntary compliance. These subpoenas, properly issued pursuant to and in furtherance of the legislature's core oversight function, have nevertheless been attacked by the media, are subject to pending litigation, threats of more litigation, and have involved nationwide attention and the work of out-of-state partisan attorneys. Given the substantial recent history of municipal non-compliance with the LAB investigation and the plenary authority of the legislature, the Assembly and this Office are defending these subpoenas. The legislature, and the public, have a right to all available information and the testimony of election officials about elections administration in Wisconsin.

A. How This Investigation Differs from the LAB's Investigation.

The LAB, established in 1971, is authorized by Wisconsin statutes to "conduct...audits of the accounts and other *financial* records of departments to assure all *financial* transactions have been made in a legal and proper manner." Wis. Stat. § 13.94(1) (emphasis added). LAB has a large staff and a laudable history of working with all state instrumentalities, but its relatively narrow mission is to ensure taxpayer money is well-spent. Its report issued October 22, 2021, notes up-front that it is concerned with "audits and evaluations of public finances and the management of public programs." As such, its interest is neither in addressing policy concerns nor the concerns of the full legislature, but of responding to directed audits of the "records of each department" of the state of Wisconsin. Further, as the recommendations in the LAB report suggest, its ability to make recommendations is statutorily limited to the four corners of current Wisconsin law and it does not generally make recommendations to improve the law. When it does, as

in the case of the current report, these changes are extraordinarily modest, perhaps recognizing its limited authorization. Finally, its sole product is a "detailed report" to the legislature, which includes discussion of any "illegal or improper expenditures." To the extent illegal or improper conduct does not implicate the state fisc, that conduct is beyond the purview of LAB inquiry.

By contrast, my Office's investigation has a wide mandate to investigate elections in Wisconsin, beyond mere "waste, fraud, and abuse," as well as the authority to gain access to necessary testimony and documents, even when recalcitrant individuals or municipalities are not otherwise inclined to "cooperate."

Can Private Groups be Involved in Running Wisconsin Elections?: Delegation and Undue Corporate Influence

While this Office draws no conclusions yet, initial interviews and discussions with clerks suggest there is widespread and substantial confusion about the appropriate role of outside money in the administration of Wisconsin elections. Evidence is already in this Office's possession indicates undue influence by well-funded private groups, who leveraged large grants to certain Wisconsin cities in order to co-opt our election apparatus to their benefit. The recent LAB investigation did not comprehensively investigate or address these concerns by clerks and the public, concerns which led to frustration and untimely resignation of at least one long-serving clerk and numerous unanswered complaints to WEC. Indeed, contracts made between outside groups and certain municipalities led directly to actions contrary to Wisconsin state law, which some clerks noted harmed both election security and the physical safety of voters. The public has a right to know if there was a *quid pro quo* arrangement between outside groups and cities, and if so, what the terms of that agreement were.

How much authority can clerks contract away to private organizations? As the LAB report contends: "Statutes do not specify the actions and responsibilities that consultants

are allowed to take at polling places and central count locations on Election Day." Nevertheless, for the purposes of legislative inquiry, this is not, and cannot, be the end of the story. Whether certain organizations and individuals operated within a grey area in state law does not preclude obtaining all relevant facts and attempting to draw fine distinctions to facilitate legislative oversight, dialogue with the public, present legislative recommendations, and restore confidence in Wisconsin's system of elections. We need to gather all facts so the legislature can address any problems.

Oblique reference to at least one major issue is made in the LAB report which bears mentioning. Specifically, the LAB report notes the following:

"We asked the clerks of all thirty-nine municipalities [that used central count locations] whether consultants worked at central count locations during the November 2020 General Election. Clerks indicated consultants associated with private organizations worked at the central count locations in two of the thirty-nine municipalities. Specifically:

- One municipality indicated a consultant attended the August 2020 primary as an observer, helped to modify the municipality's election training materials from August 2020 until October 2020, and was at the central count location on Election Day in November 2020 to provide technical assistance for electronic voting equipment. The municipality indicated at least five poll workers monitored such assistance at all times.

- A second municipality indicated a consultant provided logistical support and offered elections administration recommendations but did not have the authority to make decisions and did not count ballots. The municipality indicated the consultant initially wore a city employee identification badge at the central count location on Election Day in November 2020 but subsequently became an observer after the deputy clerk spoke with WEC's administrator about this individual."

This cursory reporting is concerning, because it substantially waters down already-public information relating to the involvement by a number of private groups in election administration, and it suggests problems were raised and adequately resolved by clerks and WEC.

In fact, in both instances, evidence is already available to this Office that is inconsistent with the LAB's report, and which indicates a more widespread and deeper issue. For example, one private organization referred to in the LAB report was directly involved in all aspects of management of election officials, was entrusted with the only sets of physical keys to the city's central count location, managed the transportation of ballots, and instructed the counting of unlawful ballots that had arrived at the central count location beyond the lawful time window.

Furthermore, under Wis. Statutes § 7.41, there are express rules for "members of the public" to exercise their right to observe Wisconsin elections, which include limitations on the ability of observers to obtain confidential voter information or to communicate with election officials. Individuals are, under Wisconsin law, either election officials or members of the public, and do not "become" observers, as the LAB report suggests. Finally, issues involving possible unauthorized access to election materials or impersonation of a municipal employee cannot be remedied by *ex parte* discussion with a single bureaucrat at WEC. None of these issues are directly addressed by the LAB report.

The LAB report also fails to address to what degree state instrumentalities may properly contract with private groups for purposes of administering public elections. Clerks have already raised concerns to this Office that there are certain election administration functions which they are simply unable to perform. Clerks and the public have raised concerns about the ability of outside contractors to legally bind election officials with onerous contractual terms.

Contracts with private groups for election administration and management.

This Office is reviewing contracts between municipalities and private groups which gave preferential access to voter data to those private groups and prohibited contracting municipalities from exercising their legal right to change election procedures, lest they be on the hook for paying substantial sums of money back to those groups. Clerks have also raised concerns about technical contracts which limit their ability to review the inner workings of equipment and software related to voter registration and vote tabulation.

A major concern raised by numerous members of the public is whether outside contractors abided by all applicable state and federal antidiscrimination laws, a question not addressed in the LAB report.

This Office has also already uncovered evidence of selective targeting of voters by these private groups, raising questions as to what extent nonpartisan government agencies were turned into partisan get-out-the-vote operations, or whether this targeting was performed on any other unlawful basis. Some of this targeting was apparently in the context of recommending ballot "drop boxes" in certain locations, but not others, a violation of Wisconsin Stat. § 6.855 (see below). Each of these facts, if true, are concerning, and this Office continues to investigate the extent of this entanglement. Furthermore, without statutorily mandated training for clerks, the possibility of undue outside influence in our elections increases. In the vacuum created by WEC, understaffed and overworked clerks can find it all-too-easy to take money and personnel from private groups that might not have compliance with the law as their top priority.

Some clerks have noted to this office the complexity and scope of Wisconsin elections will *always* and *necessarily* require delegation of at least some election functions to private companies. But clerks have suggested a line must be drawn somewhere and many express concern over the 2020 election. Indeed, one current clerk specifically recommended to this Office that private money be prohibited. This Office continues to

investigate precisely how much authority was ceded to private entities and whether that subservience hindered the fair administration of elections and/or diminished public confidence in that fairness.

Who Runs Wisconsin Elections? Finger-Pointing and the Wisconsin Elections Commission

Clerk Authority

The core of the constitutional and statutory responsibility for election administration in Wisconsin resides with county and municipal clerks. Under Wisconsin Statute § 7.15(1), the municipal clerk has "charge and supervision" of not only state, but also federal elections within a municipality. In turn, these municipal clerks report electoral results to the county clerk and provide county clerks with all materials the county clerks need to discharge their lawful duty to administer elections in their county. While municipal clerks are appointed by political officials such as mayors, county clerks in our state are directly elected.

Government Accountability Board Scandal and Creation of Wisconsin Elections Commission

To assist with developing best practices, the Wisconsin Elections Commission (WEC) was established in 2016. Prior to 2016, a large, opaque, politically partisan, and unaccountable agency, the Government Accountability Board (GAB), was charged with administering vast swaths of statewide ethics and election law. In the wake of a major statewide scandal that drew national attention, the John Doe investigations, the legislature and Governor took the unprecedented step of abolishing that agency and amending state election laws. However, rather than returning the state to a system of clear delegations of authority and broad clerk autonomy, those amendments created WEC, drawing criticism from many quarters, including Kevin Kennedy, the outgoing Director of GAB, who remarked that

the new system **would have essentially no changes, and that the new system would be "no more transparent" than the old one.**

One example of Kennedy's fulfilled prophecy is the abundance of inconsistent information relating to voter data in the registration database. In its waning days of 2015, the GAB was confronted with 28,906 voters whose information about their name and address as reported to the DMV was inconsistent with information for the same voter in the voter registration database. The GAB dismissed those concerns. However, as of 2021, those same numbers not only continue to exist and have never been adequately explained but increased in number under WEC's tenure.

Pursuant to Wisconsin law, WEC is tasked with certain portions of "the administration of...laws relating to elections." Wisconsin Statutes § 5.05(1). Precisely how far this delegation goes is an open question. WEC authority as expressly laid out in that section contemplates public rulemaking, investigation, and enforcement. However, the election code sections over which WEC has regulatory authority include numerous provisions which expressly delegate authority to individual actors, such as county and municipal clerks. In fact, Wisconsin law delegates to the "board" the duty to certify the state's electors in a presidential election, a job fulfilled in 2020 solely by the Chairperson of WEC, without board vote. *Compare* Wis. Stat. § 7.70(5). The LAB report does not make an effort to systematically review these delegations but does note in several places the "shared" election administration responsibilities.

Confusion about WEC Authority

While this Office draws no conclusions yet, initial interviews with clerks suggest there is widespread confusion about the lawful role of WEC in the state, and concern that WEC has acted outside its lawful purview. There is evidence numerous complaints by clerks to WEC were ignored. This problem is exacerbated by a lack of clarity as to the legal status of WEC guidance: some clerks are convinced compliance with WEC guidance

provides them with a legal "safe harbor" in the event the Clerk's directives consistent with the guidance are challenged in court. In a recent statement, WEC expressly disavowed that its actions could provide a basis for a defense but instead opined that it is the clerks who bear all the responsibility for election related litigation.

Additionally, WEC guidance, such as online FAQs, are apparently issued without a full Commission vote. Other documents, as the LAB report notes in the case of the March 2020 Commission-approved guidance regarding Special Voting Deputies are flatly contrary to law. As noted above, much authority is delegated to the WEC administrator. Importantly, under Wisconsin law, there is slight legal recourse other than a petition to WEC to challenge such unlawful behavior. When WEC implicitly or explicitly authorizes actions contrary to Wisconsin law, such as enabling poor security for access to statewide voter registration data systems or authorizing "shortcuts" such as issuing absentee ballots without applications or enabling widespread ballot curing, voters and candidates are left with no choice but to file expensive and time-consuming lawsuits. The LAB report, consistent with the LAB mission discussed above, did not investigate these issues, which this Office continues to investigate and collate.

Lack of Legal Remedies

Furthermore, the LAB did not investigate various decisions WEC and others made in the run-up to the 2020 election, some of which appear designed to prevent the Wisconsin courts, including the Wisconsin Supreme Court, from weighing in. Specifically, the decision by WEC to quickly issue ballots without a Green Party candidate was the determining factor in the Wisconsin Supreme Court declining to address the merits of that exclusion. WEC's action was of dubious legality. In the 2020 case of *Hawkins v. Wisconsin Elections Commission*, the 4-3 majority held that because WEC had claimed it had already issued an unknown number of ballots, there was no time to properly address the claims of the excluded Green Party candidate. In other words, WEC's own actions operated to neuter the ability of our state's highest court to address whether WEC's

actions were lawful and to provide a remedy if they were not. Then Chief Justice Patience D. Roggensack wrote a forthright dissent, noting "The court's silence not only affirms lawless conduct by the Commission, but also provides no directive for the required treatment of nomination papers in the future." This Office continues to formulate legislative options to ensure this remedial gap in Wisconsin law is repaired.

Absentee Balloting

A second action has evaded both LAB and state judicial review andinvolves the issue of absentee balloting. Precisely what rules govern the requirements for mail-in and in-person absentee voting in the state of Wisconsin? It is clear in some instances the safeguards mandated for the protection of honest absentee ballots were ignored by WEC.

Many of these safeguards were apparently abrogated by WEC and municipalities in 2020, with COVID-19 as a proffered excuse. One issue involved the illegal mass self-certification of individuals as "indefinitely confined" under the statute, a category which enables a voter to evade state voter ID requirements, but which is intended to apply to physically or physiologically immobile residents confined to their home because of their condition. Presented to the Wisconsin Supreme Court, again the majority ducked a ruling on the merits, prompting then Chief Justice Roggensack to note that it appears the Court "cannot be bothered with addressing what the statutes require to assure absentee ballots are lawfully cast." It is up to the state legislature to investigate if, how, and why state law was not followed and take legislative action.

One major issue identified involves "Democracy in the Park," which were citywide events in Madison before the election exclusively related to absentee ballots. The LAB report mentions this issue in passing as a "Special Event" occurring in a "specified outdoor setting." Without explaining the issue, the report recommends the Legislature "clarify" statutes so individuals know whether or not they can engage in absentee ballot activities contrary to the procedures laid down in Wis. Stat. § 6.855. In other words, the

LAB report implicitly notes the statutes were violated by Democracy in the Park and recommends the law be changed.

What was Democracy in the Park, and why has it been the subject of numerous citizen complaints, lawsuits, and legislative inquiries apart from this Office's investigation?

While this Office draws no conclusions, we possess evidence that the events, which occurred on September 26 and October 3, 2020, involved numerous possible violations of state law, calling into question the validity of over 17,000 absentee ballots. Specifically, these involved large outdoor gatherings where purported designees of the City Clerk's office assisted with absentee ballots that yielded over 17,000 votes. Furthermore, it is not clear that all of the workers at those events were properly deputized and trained, swore and filed the mandatory oath of office, or documents related to absentee ballots were properly handled. Finally, this Office also seeks to review the processing of those ballots. Each of these fact-intensive avenues of inquiry are crucial for determining what was improper and how to prevent future impropriety in absentee voting.

Clerk Training

In addition, this office has obtained evidence that WEC failed to complete its statutorily mandated training duties. As the LAB report notes, Wisconsin Statutes § 12.01 *et seq.*, lays out training protocols for clerks. But county clerks are politically accountable to their voters, and WEC certification or lack of certification does not affect a clerk's legal rights. However, if a clerk is *not* certificated by WEC, such as for failing to be properly trained, WEC is required by law to notify the "governing body" of that clerk's county or municipality. In other words, WEC is mandated by law to train clerks, and clerks who fail to complete training are reported by letter to the mayor or county board. Yet, as the LAB found, at least 17.5% of clerks were not properly trained, and no letters from WEC went out notifying cities and boards about the failure to complete training. This Office continues to review the issue. Moreover, this Office already has ample evidence that in

the absence of this legally mandated training, certain private groups filled the vacuum, perhaps for their own, self-interested purposes, providing some municipalities with incorrect and even unlawful advice. In a statement, at least one clerk has noted outside advice negatively impacted the security of the vote and the physical safety of voters.

Exploitation of Elders

This Office continues to review the issues involving WEC more generally, as well as other plain rules that are apparently without remedy in Wisconsin law, such as the editing of ballot applications by clerks and voting procedures at nursing homes. A recent investigation and report by the Racine County Sheriff's Office highlighted the exploitation of some of our most vulnerable citizens. Furthermore, complaints were apparently made to WEC and ignored, in a system which the sheriff described as leading to our election system being "not just broken, but shattered." I believe many Wisconsinites share the Sheriff's sentiment. It is my hope a continued investigation and final report from this Office will help change those perspectives and sentiments.

In the run-up to the November 3, 2020, election, clerks and WEC took numerous steps to alleviate public fears about COVID-19. But in this perceived crisis there was the opportunity for electoral partisan advantage. For example, Wisconsin law mandates individuals in various types of communal living facilities may have special access to absentee voting in person, but only subject to the rules of § 6.875. These rules govern the "Special Voting Deputies" that a municipality may, in turn, train and authorize to collect absentee votes in person: this is the *only* lawful method for collecting absentee ballots outside normal procedures, as Special Voting Deputies swear an oath and become duly authorized "election officials." Without the availability of Special Voting Deputies under the statute, it would be much more difficult for many senior citizens or those in assisted living facilities to vote. Yet in 2020, at the recommendation of its top administrator, WEC voted to unilaterally prohibit the use of Special Voting Deputies, explaining that COVID-19 made it too dangerous to allow for Special Voting Deputies to enter these facilities.

This Office has evidence that WEC and some clerks instructed residential care employees to act in a manner prohibited by law, collecting and assisting in completing ballots for individuals in these group facilities, including those with dementia. This led to record-high voting by individuals who had not voted for nearly a decade and may have lacked the cognitive ability to vote.

On its face, this type of activity could lead to criminal referral for the residential care employees, as the Chairperson of WEC has suggested. But residential care staff represent the "little fish" in this alleged criminal enterprise. This Office is reviewing the relevant Wisconsin statutes to facilitate the criminal referral process and make legislative recommendations. This includes reviewing legal methods for ensuring our senior citizens are not bullied or taken advantage of, and neither nursing homes nor their residents are used for any unlawful election activity, merely because these citizens are vulnerable, easy targets for partisan predators.

WEC: Self-Policing and Self-Serving

Numerous members of the public, as well as the clerks, have questioned the independent authority clerks have to administer an election consistent with state law in light of WEC's guidance, which in several instances was contrary to those voting laws. Some clerks feel WEC may legally bind the clerks in granular decisions about their local needs. Other clerks are concerned about repercussions for not following WEC guidance. Many clerks have expressed disagreement with WEC conclusions, and some have done so publicly. Numerous members of the public have raised concerns about WEC's ability to police itself: the discretionary nature of WEC intake, review, and response to complaints, and the fact that complaints about WEC are handled—or not handled, as the case may be—by WEC itself.

This Office continues to interview clerks and expects to discuss with WEC staff precise nature of WEC's role in future Wisconsin elections.

How can the Public be Confident in Our Elections? The Black Box

As former GAB Director Kevin Kennedy noted, the new WEC system is, apparently, "no more transparent" than the old one which he ran. Without robust legislative oversight, many Wisconsinites are at risk of feeling their vote does not count, or that there is widespread election fraud in the state. Worse, their fears may be well-grounded. Two major areas of inquiry are being looked at by my Office, both dealing with the appropriate level of transparency for our election systems. First, my Office is reviewing the laws and procedures relating to the use of technological tools in administering elections: the "voting machines" and the various election databases used by WEC. Second, my Office is reviewing barriers to public access to information, such as excessive charges for public access to public registration data.

While this Office draws no conclusions, interviews with clerks, citizens, and other groups suggest there is widespread concern about the inability of an average citizen to track how elections are run. This inability has huge downstream consequences, as citizens are often presented with snippets of information reminiscent of the "confusopoly" in health insurance. Presented with outdated data sets of dubious accuracy, citizens seeking to use public information to confirm election results are unable to do so, while those with money and access (or preferential contracts, as noted above) can access better data, more quickly. Further, the precise operations of voting machines are not readily accessible or understood by the public, or by commissioners on WEC itself. As with health insurance, the system operates on autopilot, with the insured praying their bill is accurate, and with voters praying the system is working as it is supposed to.

Election systems in Wisconsin are governed by state and federal law. Specifically, the federal Election Assistance Commission (EAC) created under the Help America Vote Act

of 2002 (HAVA) is tasked with approving all voting systems used in federal elections, and with approving all modifications of voting systems used in federal elections. 52 U.S.C. § 20971. As a part of this, voting systems vendors submit their proposed systems to the EAC for approval. Typically, once a system is tested and approved by the EAC, the vendor will make a similar application to WEC, which may approve the system for sale and use within the state of Wisconsin. However, beginning in 2015 the state of Wisconsin allowed GAB (and now WEC) to approve systems for use in the state which are not approved by the EAC. Wis. Stat. § 5.591. While there is thus wide discretion vested in WEC to approve changes to voting systems, federal law mandates that "all records and papers... relating to any application, registration, payment of poll tax, or other act requisite to voting in such election" be preserved by the State for twenty-two months following the election. 52 U.S.C. § 20701.

But as was made eminently clear in a recent WEC meeting held after a preservation request issued by this Office, WEC officials and staff are not at all clear as to what "modifications" to voting machines require WEC approval, which modifications can lawfully be made, or what certain software updates actually entail. Further, WEC approval of actions that might violate federal record keeping laws are no guarantee of legal immunity for clerks with final say over what happens to voting machines in their locales. In fact, as one machine vendor noted during that open meeting, in order to install a software update, that company would be obliged to entirely "wipe" a machine. That is, to delete all information from election hardware. Whether this technical process destroys election records in contravention of federal law is a question that WEC has yet been unable to answer.

In order to address this and related questions, this Office has been allocated a budget to engage neutral, certificated data security experts, and has already taken steps to initiate an open and full technical audit of various voting systems to understand and report on the security of these systems. Whatever the results, various clerks have already suggested they themselves do not know precisely how the voting machines work and

rely entirely upon private contractors to assure them of system integrity. This in and of itself may be a problem. The problem is further exacerbated in that WEC, who is responsible for training the clerks on the machines, may not itself know how the machines work.

Prior to the establishment of this Office, the Special Counsel did personally engage with various outside individuals relating to various voting machine concerns. This Office neither endorses the views of any particular outside individual nor has this Office yet uncovered any evidence of foreign hacking of elections in the state of Wisconsin. Nevertheless, the opacity of elections systems has given rise to numerous theories and concerns about the 2020 election.

A second issue related to the transparency of our election system in the state is the public availability of voter data. While this Office as yet draws no conclusions, there is already evidence that security surrounding the WisVote (SVRS) system is lax. This statewide system enables clerks to track absentee ballot requests and includes highly sensitive personal information. As such, it is supposed to be subject to a high level of security laid out in WEC guidance. Nevertheless, there is already some evidence of unauthorized access to this database. Further, several clerks have complained that they were provided by WEC with numerous, unrequested access keys, leading to a security headache and concerns that the statewide system was not secure.

In addition to concerns about too much access, concerns have been raised about not enough access, or about unequal access, to voter registration information. This is important because access to this data is necessary for tracking the accuracy of reported election results. WEC does provide statewide voter registration data for a fee up to, and usually, $12,500. This fee is set by WEC administrative rule, and it is mandated by statute that the fee be set "at an amount estimated to cover both the cost of reproduction and the cost of maintaining the list at the state and local level." Wis. Stat. § 6.36(6). Nevertheless, it is apparently the case that the fee is charged for each reproduction, no matter the actual

cost, and that subsequent individuals requesting a list that has already been produced are charged the same rack-rate. Further, there is some evidence that outside groups were provided privileged access to this data without fee, and on an expedited basis. This Office continues to investigate this matter, and again, this issue is not addressed in the LAB report.

Conclusion

The people of the state of Wisconsin have a right to know how our elections are run. The legislature has the common law and constitutional right and obligation to investigate how our state laws are being administered. Without adequate information and oversight, citizens in a democracy justifiably lose confidence that their vote counts and their system of government is working properly.

This Interim Report seeks to build upon the good work of many citizens and government officials including the vast majority of county and municipal clerks, and to shine a light on issues and concerns of interest. It is a healthy exercise in good government, not an attempt to overturn any election. As this investigation continues, my Office will vigorously seek out and obtain all available truthful information, so that it can present this information to the public and to the Assembly.

If, in the course of this investigation, the Office obtains information that could be used in a criminal prosecution, this Office will cooperate fully with all appropriate law enforcement entities.

EXHIBIT 20

Cyber Ninjas, Maricopa County Forensic Election Audit, vol. III
(Sept. 24, 2021)

9/24/2021

Maricopa County Forensic Election Audit

Volume III: Result Details

Work Performed For:
Arizona State Senate
1700 W Washington St
Phoenix, AZ 85007

Cyber Ninjas
Phone: (941) 3-NINJAS
Fax: (941) 364-6527
www.CyberNinjas.com
5077 Fruitville Rd #109-421, Sarasota, FL 34232

1 Contact Details

Name	Title	Phone	E-mail
Doug Logan	Principal Consultant	941-364-6527	dlogan@CyberNinjas.com

2 Table of Contents

1 Contact Details 1
3 Document Overview 2
4 Tally Results 2
4.1 Presidential Race 2
4.2 Senate Race 3
5 Voter History, Ballot, and Certified Results Findings 3
5.1 Ballot Scoring Methodology 3
5.2 Finding Summary Table 4
5.3 Critical Findings 5
5.4 High 7
5.5 Medium Findings 10
5.6 Low Findings 19
5.7 Informational Findings 47
6 Voting Machine Findings 61
6.1 Voting Machine Scoring 61
6.2 Digital Analysis Summary 61
6.3 Findings Summary Table 61
6.4 High Findings 62
6.5 Medium Finding 72
7.6 Low Findings 91
7 About Cyber Ninjas 96

3 Document Overview

The audit was designed to be a comprehensive review of the results from the Maricopa County 2020 General Election to confirm the effectiveness of existing legislation in governing elections, and to provide additional insights on possible areas of information-based legislative reform that could ensure an even greater level of integrity and accuracy in how elections are conducted.

This audit is the most comprehensive election audit that has been conducted. It involved reviewing everything from the voter history for the election, to retallying all 2.1 million ballots by hand, to performing forensic photography and review of the ballot paper, to conducting cyber forensic imaging and analysis of the provided voting equipment. This extensive process involved over 1,500 people who contributed a total of over 100,000 hours of time over the course of more than five months from when setup began, to when this report is completed.

This volume of the report serves to outline details of the results from the audit; including all the data and evidence to support the conclusions of this report.

4 Tally Results

The audit included a full hand-recount of all 2.1 million ballots from the 2020 General Election. During this process all original ballots were counted, as well as those ballots returned from duplication. Ballots that were duplicated included various categories of ballots that were not able to be run through the voting machines, such as damaged ballots or Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) ballots. The tallies from the original ballots sent to duplication, and the ballots received back from duplication were kept separate so that a comparison could occur. As can be found in audit finding, “More Duplicates Than Originals,” there were more duplicates than there were originals. For this reason, we utilized the counts of the originals for all official tallies.

This is the most important finding in the audit because the paper ballots are the best evidence of voter intent, and there is no reliable evidence that the paper ballots were altered to any material degree.

4.1 Presidential Race

The chart below summarizes the results of the hand-recount of the Presidential Race of the Maricopa County Forensic Audit. These tallies are based on the tallies from all original ballots and does not include the ballots duplicated from the originals.

	Trump	Biden	Jorgenson	Write In / Over / Under	Total
Maricopa County Forensic Audit	995,404	1,040,873	31,501	20,791	2,088,569
Official Maricopa County Canvass	995,665	1,040,774	31,705	21,419	2,089,563
DELTA	(261)	99	(204)	(628)	(994)

4.3 Senate Race

The chart below summarizes the results of the hand-recount of the Senate Race of the Maricopa County Forensic Audit. These tallies are based on the tallies from all original ballots and does not include the ballots duplicated from the originals.

NOTE: Vote totals for the presidential and senatorial elections mismatch slightly primarily due to small differences in hand counts among the 2.1M million ballots.

	McSally	Kelly	Write In / Over / Under	Total
Maricopa County Forensic Audit	983,662	1,064,336	40,398	2,088,396
Official Maricopa County Canvass	984,203	1,064,396	40,964	2,089,563
DELTA	(541)	(60)	(566)	(1,167)

5 Voter History, Ballot, and Certified Results Findings

The following section outlines all findings related to voting history, ballots and the certified results. This section covers everything that directly impacts the counting and accounting of results.

5.1 Ballot Scoring Methodology

Ballot related findings are scored based on the total number of potential ballots impacted by the finding. Based on the range by which this falls within a Severity is assigned, as can be seen in the chart to the right. In these circumstances a severity will still be assigned to the finding based on the potential impact the finding may have had on the election.

Ballots Impacted	Severity
10,000+	Critical
5,000 – 9,999	High
1,500 – 4,999	Medium
Less than 1,500	Low

5.2 Finding Summary Table

#	Finding Name	Phase	Ballots Impacted	Severity
5.3.1	Mail-in Ballots Voted from Prior Address	Voter History	23,344	Critical
5.4.1	More Ballots Returned by Voter Than Received	Voter History	9,041	High
5.4.2	Voters That Potentially Voted in Multiple Counties	Certified Results	5,295	High
5.5.1	Official Results Does Not Match Who Voted	Certified Results	3,432	Medium
5.5.2	More Duplicates Than Original Ballots	Ballot	2,592	Medium
5.5.3	In-Person Voters Who Had Moved out of Maricopa County	Certified Results	2,382	Medium
5.5.4	Voters Moved Out-of-State During 29-Day Period Preceding Election	Voter History	2,081	Medium
5.5.5	Votes Counted in Excess of Voters Who Voted	Certified results	1,551	Medium
5.6.1	Voters Not Part of the Official Precinct Register	Voter History	618	Low
5.6.2	Duplicated Ballots Incorrect & Missing Serial Numbers	Certified Results	500	Low
5.6.3	Ballots Returned Not in the Final Voted File	Ballot	430	Low
5.6.4	Mail-in Ballot Received Without Record of Being Sent	Certified Results	397	Low
5.6.5	Voters With Incomplete Names	Voter History	393	Low
5.6.6	Deceased Voters	Voter History	282	Low
5.6.7	Audit UOCAVA Count Does Not Match the EAC Count	Ballots	226	Low
5.6.8	Late Registered Voters with Counted Votes	Voter History	198	Low
5.6.9	Date of Registration Changes to Earlier Date	Voter History	194	Low
5.6.10	Duplicate Voter IDs	Voter History	186	Low
5.6.11	Mulitple Voters Linked by AFFSEQ	Voter History	101	Low
5.6.12	Double Scanned & Counted ballots	Ballot	50	Low
5.6.13	UOCAVA Electronic Ballots Double Counted	Ballot	6	Low
5.6.14	Duplicate Ballots Reuse Serial Numbers	Ballot	6	Low
5.7.1	Audit Interference	Ballot	N/A	Informational
5.7.2	Batch Discrepancies	Ballot	N/A	Informational
5.7.3	Commingled Damaged and Original Ballots	Ballot	N/A	Informational
5.7.4	Early Votes Not Accounted for in EV33	Certified Results	N/A	Informational
5.7.5	High Bleed-Through Rates on Ballots	Ballot	N/A	Informational
5.7.6	Improper Paper Utilized	Ballot	N/A	Informational
5.7.7	Inaccurate Identification of UOCAVA Ballots	Ballot	N/A	Informational
5.7.8	Missing Subpoena Items	Ballot	N/A	Informational
5.7.9	No Record of Voters in Commercial Database	Voter History	N/A	Informational
5.7.10	Out of Calibration Ballot Printers	Ballot	N/A	Informational
5.7.11	Real-Time Provisional Ballots	Voter History	N/A	Informational
5.7.12	Voter Registration System Audit Access	Voter History	N/A	Informational
5.7.13	Questionable Ballots	Ballot	N/A	Informational

5.3 Critical Findings

5.3.1 Mail-in Ballots Voted from Prior Address

Ballots Impacted 23,344

Mail-in ballots were cast under voter registration IDs for people that may not have received their ballots by mail because they had moved, and no one with the same last name remained at the address. Through extensive data analysis we have discovered approximately 23,344 votes that may have met this condition. If a registered voter does not have a secondary mailing address listed with the county and no longer lives at the address listed on their voter registration, they should not receive their mail-in ballot by automatic postal forwarding. In certain circumstances, however, it may be possible for them to receive a ballot, for example, if they know the present occupant, or if the ballot is improperly forwarded.

If ballots are being sent by forwardable mail, this would violate the Arizona Elections Procedures Manual, which requires, "A ballot-by-mail must be mailed to voters by first-class, non-forwardable mail." EPM p. 56. Therefore, this is a potentially criminal act. *See* ARS 16-452(C) (any person who violates a rule set forth in the EPM "is guilty of a class 2 misdemeanor.").

Ensuring that ballots are sent by non-forwardable mail serves an important purpose. When non-forwardable mail is returned undelivered, the County Recorder is required to initiate a process that places a voter on inactive status - meaning they will no longer automatically receive an early ballot - and may eventually remove them from the rolls entirely. ARS 16-165(A)(7), 544(E).[1]

The Final Voted File, or VM55, was cross-checked against a commercially available data source provided by Melissa[2] called Personator. Personator is a best-in-class identity and address validation tool. It confirms that an individual is associated with an address, indicates prior and current addresses, tracks when and where the individual moves, tracks date-of-birth and date-of-death. To accomplish this, it utilized both private and government data sources such as the US Postal Service's National Change of Address (NCOA) service, and the Social Security Administration's Master Death List.

Addresses were not included in the results if there was a valid secondary mailing address as part of the voting record. Only moves prior to October 5, 2020, are included in the move numbers.

NOTE: The following chart illustrates the percentage of voters by registered party that the Ballot Impacted number represents. This should give a rough idea on the impact to the electorate if the votes were cast by the voters and not another individual that was somehow able to gain access to the mail-in ballot.

Party	%
Democrat Party	39.5%
Republican Party	33.0%
Prefer Not to Declare	26.5%
Libertarian Party	1.0%

NOTE: While high quality commercial database sources were utilized to assemble these findings, some error is expected within these results. To further validate these findings, it is recommended that canvassing be conducted.

[1] With the passage of SB 1485, going forward, voters may be removed from the rolls if they have not voted for a prolonged period of time.

[2] https://www.melissa.com

NOTE: A full list of the Voter IDs affected can be found in esB1-B3 There are potential ways that a voter could receive their ballot which in some cases would not violate the law. Additional investigation by the Attorney General is recommended for any conclusive determination.

Description	Ballots
Mail-in votes from voters who moved within Maricopa County prior to the registration deadline	15,035
Mail-in votes from voters who moved out of Arizona prior to registration deadline	6,591
Mail-in votes from voters who moved within Arizona but out of Maricopa prior to registration deadline	1,718

NOTE: Please see Appendixes B1, B2 and B3 for the details for this finding.

5.3.1.1 References

- A.R.S. § 16-101 – Qualifications of registrant[3]
- State of Arizona – 2019 Elections Procedures Manual[4]
- A.R.S. § 16-165 – Causes for Cancellation[5]
- A.R.S § 16-452 – Rules[6]
- A.R.S § 16-544 – Permanent early voting list[7]

5.3.1.2 Data Files Utilized

File Name	MD5 Hash
Maricopa County-VM55 Final Voted Nov2020 PBRQ	43070bc7afdf40a37cd45092e9733654

5.3.1.3 Recommendation

Legislation should be considered that links voter roll registration to changes in driver's licenses or other state identification, as well as requiring the current voter rolls be validated against the United States Postal Service (USPS) National Change of Address (NCOA) at a predefined period prior to every election.

Laws already exist for interstate reporting of changes in residence, addresses, and driver's licenses. Tying voter roll registration to these forms of identification would greatly increase the likelihood that voter registration details would be kept up to date. Individuals are more likely to remember their license needs to be updated immediately than voter registration, and since all states now offer the ability to register to vote when getting a license, license updates could also update voter rolls.

[3] https://www.azleg.gov/ars/16/00101.htm
[4] https://azsos.gov/sites/default/files/2019_ELECTIONS_PROCEDURES_MANUAL_APPROVED.pdf
[5] https://www.azleg.gov/ars/16/00165.htm
[6] https://www.azleg.gov/ars/16/00452.htm
[7] https://www.azleg.gov/ars/16/00544.htm

It is recommended that the voter rolls be validated against the NCOA both 90 days or more prior to the election, in addition to a week before mail-in ballots are sent out. This check would be utilized to determine if a mail-in ballot would be sent to the address since ballots are not allowed to be forwarded. The legislature may want to consider whether a change of address should suspend Permanent Early Voting List (PEVL) enrollment.

The Senate should consider referring this matter to the Attorney General's Office for a criminal investigation as to whether the requirements of ARS 16-452(C) have been violated.

5.4 High

5.4.1 More Ballots Returned by Voter Than Received

Ballots Impacted 9,041

9,041 more ballots show as returned in the EV33 Early Voting Returns File for a single individual who voted by mail than show as sent to that individual within the EV32 Early Voting Sent File. In most of these instances an individual was sent one ballot but had two ballots received on different dates.

Further investigation would be needed to determine the cause, but this could be explained in any of the possible ways:

- More than one ballot could have been sent out, but an entry was missed within the EV32 file.
- The same ballot could have been processed more than once on different days, resulting in two EV33s for one ballot.
- Checking into Early Vote in person may not have recognized that a mail-in ballot was already received and both the Early Vote In-Person and the mail-in may have generated an EV33.
- A counterfeit ballot was sent via mail and both the legitimate ballot sent and the counterfeit ballot generated EV33 entries.

NOTE: We've been informed shortly before the release of this report that some of the discrepancies outlined could be due to the protected voter list. This has not been able to be validated at this time, but we thought it was important to disclose this information for accuracy.

NOTE: An EV33 indicates that a ballot is received and does not necessarily mean the ballot was counted. It is assumed that only the first ballot received and validated is counted.

Ballots Sent to Voter	Ballots Received for Voter	Quantity of Voters
1	2	8,875
1	3	163
1	4	3

NOTE: Please see Appendix C1 for details on the voters who had more ballots received than sent.

NOTE: The following chart illustrates the percentage of voters by registered party that the Ballot Impacted number represents. This should give a rough idea on the impact to the electorate if the votes were cast by the voters and not another party that was somehow able to cast a vote.

Party	%
Democrat Party	34.4%
Republican Party	30.4%
Prefer Not to Declare	30.1%
Independent	3.7%
Libertarian Party	1.3%

5.4.1.1 REFERENCES

- A.R.S. § 16-246 – Early Balloting[8]
- A.R.S. § 16-542 – Request for ballot[9]
- A.R.S § 16-544 – Permanent early voting list[10]
- A.R.S. § 16-558.01 – Mailing of Ballots[11]

5.4.1.2 DATA FILES UTILIZED

File Name	MD5 Hash
Maricopa County-VM55 Final Voted Nov2020 PBRQ	43070bc7afdf40a37cd45092e9733654
EV33-1377-10-09-2020_101111.txt	f1daa7089f7300237f6b4ff779661cf9
EV33-1377-10-12-2020_113210.txt	72e4e6c102e3539b4dd15b4454357b69
EV33-1377-10-13-2020_111553.txt	9b14841281c031533322b50aabb86a24
EV33-1377-10-14-2020_112757.txt	1b7537d7d9b927dbf4e462ed5ee8f97c
EV33-1377-10-15-2020_121331.txt	dec7d08dde4970c26e32b8c844f4a9ab
EV33-1377-10-16-2020_113522.txt	f0a632c3fd9b5f177d48504dc119be31
EV33-1377-10-19-2020_111708.txt	db80b692a9188add0844a8974e227287
EV33-1377-10-20-2020_112351.txt	57d1795db8be71d516e29350e347fb3a
EV33-1377-10-21-2020_111843.txt	56c3b5a11651c68735164c578eade4e1
EV33-1377-10-22-2020_111714.txt	03551f170bf758efc90c013d0fe2e467
EV33-1377-10-23-2020_112614.txt	dbfdd369ac148723540c83f614cca454
EV33-1377-10-26-2020_111318.txt	0b68adff779f59c70a530000bf989aca
EV33-1377-10-27-2020_111413.txt	a6fc7377bf6c6fe6653f539c5970a6f7
EV33-1377-10-28-2020_111331.txt	43758b9290f90d0305d5ed84aa10becb
EV33-1377-10-29-2020_111300.txt	410b30b06f2ca73022f27173fe114038
EV33-1377-10-30-2020_111804.txt	5cb44e5ea214f40227e04345d4355ff7
EV33-1377-11-02-2020_111214.txt	5d15bb8686a022f53400550cfe010a07

[8] https://www.azleg.gov/ars/16/00246.htm
[9] https://www.azleg.gov/ars/16/00542.htm
[10] https://www.azleg.gov/ars/16/00544.htm
[11] https://www.azleg.gov/ars/16/00558-01.htm

File Name	MD5 Hash
EV32-1377-09-18-2020_075112.txt	ab22e9ba4ad54af1b7a47f8381d506c7
EV32-1377-09-30-2020_111728.txt	2e4df9ccf2e5e64fd7e164628ff7667a
EV32-1377-10-01-2020_113125.txt	92538fe838c7c872957d155a98290874
EV32-1377-10-02-2020_125658.txt	be7d44838daa2aa758a0adb1dfe88acd
EV32-1377-10-05-2020_112338.txt	31a356a1a1826639759fc66afb812498
EV32-1377-10-06-2020_114600.txt	cb70c4468ebd51142003e46e3e1257c4
EV32-1377-10-07-2020_111951.txt	185d423606927ba15f827e19329c02aa
EV32-1377-10-08-2020_111639.txt	4f82598b6fab071300e92b8f56407451
EV32-1377-10-09-2020_112718.txt	bdf22cce7eca5eeb0b52dbb9f87a54b6
EV32-1377-10-12-2020_113153.txt	67a7ab52ab0850127528b18667eaf5c6
EV32-1377-10-13-2020_111535.txt	81af1c0b010368d0e11cc68e8a21f2e6
EV32-1377-10-14-2020_112738.txt	e88cce6a8a27b5bf755765f516710c48
EV32-1377-10-15-2020_121305.txt	2f12b801d981afc0e4e114bdfbf4241c
EV32-1377-10-16-2020_113410.txt	46a251f88fdd1d2e2352ac1dc61fffa9
Maricopa_EV32-1377-10-19-2020_111633-2020-10-20T14 53 30Z.txt	9cd6e80c07e1f33129cf98302930abb6
Maricopa_EV32-1377-10-20-2020_112309-2020-10-21T15 13 12Z.txt	e3cc25b520b5710090f4dfff2d7fce7f
Maricopa_EV32-1377-10-21-2020_111759-2020-10-22T15 08 54Z.txt	e786fec02788d0b7c4392ca5b1cd284e
Maricopa_EV32-1377-10-22-2020_111639-2020-10-23T15 03 40Z.txt	86ea315f6bce7c0c902027b5373f6e2c
Maricopa_EV32-1377-10-23-2020_112532-2020-10-26T15 00 59Z.txt	ca42553da16ea38cf2b72f29b81a990f

5.4.1.3 Recommendation

It is recommended that the Attorney General inquire of Maricopa County as to the reason for this discrepancy, and if a sufficient explanation is not received an investigation be opened to investigate this further.

5.4.2 Voters that Potentially Voted in Multiple Counties

Ballots Impacted 5,295

Comparing the Maricopa County VM55 Final Voted File to the equivalent files of the other fourteen Arizona counties resulted in 5,047 voters with the same first, middle, last name and birth year, representing 10,342 votes among all the counties. While it is possible for multiple individuals to share all these details, it is not common although the incidence here (roughly one-third of one percent) may be the rate of commonalities in identifying information between legitimate, separate individual voters especially with common last names. This list should be fully reviewed.

NOTE: The Ballot Impacted was calculated by the total number of votes (10,342) and subtracting the number of maximum number of potential unique people (5,047). This yielded 5,295.

NOTE: Please see Appendix D1 for details on the potential voters who cast a vote in more than one location.

5.4.2.1 References

- State of Arizona – 2019 Elections Procedures Manual[12]
- A.R.S. § 16-120 – Eligibility to vote[13]

5.4.2.2 Data Files Utilized

File Name	MD5 Hash
Maricopa County-VM55 Final Voted Nov2020 PBRQ	43070bc7afdf40a37cd45092e9733654
Apache County - 01_02_2021 Party CD-2021-02-09T00 22 11Z.csv	be4c0af2563848085d58ba6b35a486d9
Cochise County Voter File 01022021.csv	6839d6c54e5da7b5440018b23c239a80
Coconino County - 11-3-20 General Voter List with Voting History.csv	aa92299b3af0188e0d477d30929ff2e8
Gila County - votinghistoryexport_637454437931504987.csv	ea8475adc98ba6d488c1cf772333c750
Graham County - votinghistoryexport022021.csv	a967c66261fc118b12a7673cfc140293
Greenlee Party Report Active voters with voting history 1-6-2021-2021-01-06T17 47 47Z.csv	9f911e1249c0c6303d393e88f435057c
La Paz County - votinghistoryexport11032020-2020-12-09T19 37 25Z.csv	a94f953df2f4843ee1a753f2102ef589
Mojave County - Party File 1-2-2021.csv	427dfa3347df1c9a373d1c60250d71d3
Navajo County - Parties List January 21-2021-02-10T22 08 47Z.csv	1aea8fc97eaad284ba27de8689774315
Pima County - ActiveVoters20210105112009.csv	93bbfb0586d83cc714b8d02b2ad8d8e3
Pinal County - Active Voter List 01052021.csv	44d10afdac81cf1dea2bd5faffda50dc
Santa Cruz County - 1ST QTR ACTIVE VOTER LIST REPORT 01202021.csv	73e8599aab7c084c94605621f0c148e2
YavapaiCounty - 11-10-2020 votinghistory-Yavapai.csv	2e68ec2f922a0eda6999f3fc5b1c0638
Yuma County - Voting History Export_Include ALL Registered Voters.csv	d87c732fc069e85db4a92974bd7c689b

5.4.2.3 Recommendation

Legislation should be considered which requires a more clear schedule for cleaning up and maintaining voter rolls, including specific requirements for a county based on its size and growth.

5.5 Medium Findings

[12] https://azsos.gov/sites/default/files/2019_ELECTIONS_PROCEDURES_MANUAL_APPROVED.pdf
[13] https://www.azleg.gov/ars/16/00120.htm

5.5.1 Official Results Do Not Match Who Voted

Ballots Impacted 3,432

The official result totals do not match the equivalent totals from the Final Voted File (VM55). These discrepancies are significant with a total ballot delta of 11,592 between the official canvass and the VM55 file when considering both the counted and uncounted ballots.

Official Results verses Final Voted File (VM55) – Counted Ballots

Description	Type	Official Results	Final Voted (VM55)	Delta
Early Vote	Mail In (R)	N/A	1,702,981	
	In Person (B)	N/A	209,112	
	Total	1,915,487	1,912,093	3,394
Election Day Vote	Regular	167,878	N/A	
	Provisional	6,198	N/A	
	Total	174,076	(P) 174,038	38
Total Counted:		2,089,563	2,086,131	3,432

NOTE: Please see Appendix E1 for a full break-down by precinct of the differences between the Official Results and the Final Voted File (VM55).

5.5.1.1 Data Files Utilized

File Name	MD5 Hash
11-03-2020-1 Final Official Summary Report NOV2020.pdf[14]	321a78c74d4f442da0659014b29cb091
Maricopa County-VM55 Final Voted Nov2020 PBRQ	43070bc7afdf40a37cd45092e9733654

5.5.1.2 Recommendation

Legislation should be considered that would require the Official Canvass to fully reconcile with the Final Voted File. The number of individuals who showed up to vote should always match the number of votes cast.

[14] https://recorder.maricopa.gov/electionarchives/2020/11-03-2020-1%20Final%20Official%20Summary%20Report%20NOV2020.pdf

5.5.2 More Duplicates Than Original Ballots

Ballots Impacted 2,592

Maricopa County reported "In this election, Maricopa County had 27,869 duplicate ballots pertaining to the Presidential Electors."[15] The audit team counted 29,557 duplicate ballots. However, only 26,965 original ballots were sent to duplication.

Description	Ballots Count
Maricopa County Forensic Audit - Original Ballots Sent to Duplication	26,965
Maricopa County Forensic Audit – Duplicate Ballots Counted	29,557
Maricopa County – Reported Duplicate Ballots	27,869

A comparison of the total number of original ballots sent to duplication vs the total number of duplicate ballots shows that Maricopa County counted 2,592 more duplicate ballots than original ballots sent to duplication. The audit team attempted to resolve the discrepancies, but those efforts were impeded by the County's failure to properly identify duplicate ballot batches and failure to assign unique serial numbers to each damaged ballot sent to duplication and then match that number to the duplicate ballot printed to replace it.

The County reported 1688 fewer ballots sent to duplication than identified by the audit team. The County provided 904 fewer original ballots than they reportedly duplicated.

These extra duplicates favored Republican candidates over Democrat candidates, and even favored the Libertarian candidate at a higher rate than the overall vote distribution.

Description	Damaged Sent to Duplication (DSD)	Duplicate Ballots (DUP)	Expected % To Candidate	% Difference To Candidate
Trump	995,404	996,896	48%	58%
Biden	1,040,873	1,041,733	50%	33%
Jorgenson	31,501	31,580	2%	3%

Description	Damaged Sent to Duplication (DSD)	Duplicate Ballots (DUP)	Expected % To Candidate	% Difference To Candidate
McSally	983,662	985,100	47%	55%
Kelly	1,064,336	1,065,266	51%	36%

NOTE: Please see Appendixes F1 and F2 for the details of this finding.

[15] https://ecf.azd.uscourts.gov

5.5.2.1 References

- Maricopa Clerk of Court Duplicate Ballots[16]
- State of Arizona – 2019 Elections Procedures Manual[17]
- A.R.S. § 16-621 – Proceedings at the counting center[18]

5.5.2.2 Recommendation

Legislation should be considered that requires regular audits of elections within a year of the election. Among the mandatory items required to perform in the audit should be a review of the duplicate ballot process.

5.5.3 In-Person Voters Who Had Moved Out of Maricopa County

Ballots Impacted 2,382

The VM55 Final Voted File, was cross-checked against a commercially available data source provided by Melissa called Personator and 2,382 ballots were cast voter IDs for individuals that moved outside of Maricopa County prior to 10/5/2020. Personator is a best-in-class identity and address validation tool. It confirms that an individual is associated with an address, indicates prior and current addresses, tracks when and where the individual moves, tracks date-of-birth and date-of-death. To accomplish this, it utilized both private and government data sources such as the US Postal Service's National Change of Address (NCOA) service, and the Social Security Administration's Master Death List. Only moves prior to October 5, 2020, are included in the move numbers.

NOTE: While high quality commercial database sources were utilized to assemble these findings, a small percentage of error is expected within these results. To further validate these findings, it is recommended that canvassing be conducted.

Description	Ballots
In-Person votes from voters who moved out of Arizona prior to registration deadline	1,528
In-Person votes from voters who moved within Arizona but out of Maricopa prior to registration deadline	854

NOTE: Please see Appendixes G1 and G2 for additional details on the individuals that show as moved.

NOTE: The following chart illustrates the percentage of voters by registered party that the Ballot Impacted number represents. This should give a rough idea on the impact to the electorate if the votes were cast by the voters and not another party that was somehow able to cast a vote.

Party	%
Republican Party	43.37%
Democrat Party	25.06%
Prefer Not to Declare	26.87%
Independent	3.27%
Libertarian Party	1.18%
Green Party	0.25%

[16] https://www.clerkofcourt.maricopa.gov/home/showpublisheddocument/1902/637425888214000000
[17] https://azsos.gov/sites/default/files/2019_ELECTIONS_PROCEDURES_MANUAL_APPROVED.pdf
[18] https://www.azleg.gov/ars/16/00621.htm

5.5.3.1 References

- Maricopa County – 11-03-2020 - General Election Canvass Summary[19]

5.5.3.2 Data Files Utilized

File Name	MD5 Hash
Maricopa County-VM55 Final Voted Nov2020 PBRQ	43070bc7afdf40a37cd45092e9733654

5.5.3.3 Recommendation

Legislation should be considered that links voter roll registration to changes in driver's licenses or other state identification, as well as requiring the current voter rolls be validated against the United States Postal Service (USPS) National Change of Address (NCOA) at a predefined period prior to every election.

Laws already exist for interstate reporting of changes in residence, addresses, and driver's licenses. Tying voter roll registration to these forms of identification would greatly increase the likelihood that voter registration details would be kept up to date. Individuals are more likely to remember their license needs to be updated immediately than voter registration, and since most states now offer the ability to register to vote when getting a license, license updates could also update voter rolls.

It is recommended that the voter rolls be validated against the NCOA both 90 days or more prior to the election, in addition to a week before mail-in ballots are sent out. This check would be utilized to determine if a mail-in ballot would be sent to the address since ballots are not allowed to be forwarded. The legislature may want to consider whether a change of address should suspend Permanent Early Voting List (PEVL) enrollment.

[19] https://recorder.maricopa.gov/electionarchives/2020/11-03-2020-1%20Final%20Official%20Summary%20Report%20NOV2020.pdf

5.5.4 Voters Moved Out-of-State During 29-Day Period Preceding Election

Ballots Impacted 2,081

Arizona law and the 2019 Election Procedures Manual address the specific voting eligibility of a person who moves out of Arizona during the 29-day period before the election. A person that moved out of Arizona between 10/5/2020 and 11/03/2020, was no longer legally considered a "resident," however was eligible by law to vote a presidential-only ballot. See the image below taken from the 2019 Elections Procedure Manual (pg. 30).

> *ARIZONA SECRETARY OF STATE*
> *2019 ELECTIONS PROCEDURES MANUAL*
>
> If a registrant moves to a different state during the 29-day period preceding the next election, the registrant is not a qualified elector (and is therefore ineligible to vote) in Arizona. However, a registrant retains the right to vote in Arizona for President of the United States (and no other races) at the general election during a Presidential election year. A.R.S. § 16-126. Requesting a presidential-only ballot requires the County Recorder to cancel the registrant's record "promptly" following the general election. A.R.S. § 16-165(A)(6).

The 2019 Elections Procedure Manual states "A registrant is a "resident" if they have physical presence in the county along with an intent to remain. A registrant may be temporarily absent from the jurisdiction without losing their residency status, as long as they have an intent to return. A.R.S. § 16-103." (pg. 12)

The Final Voted File, or VM55, was cross-checked against a commercially available data source provided by Melissa[20] called Personator. Personator is a best-in-class identity and address validation tool. It confirms that an individual is associated with an address, indicates prior and current addresses, tracks when and where the individual moves, tracks date-of-birth and date-of-death. To accomplish this, it utilized both private and government data sources such as the US Postal Service's National Change of Address (NCOA) service, and the Social Security Administration's Master Death List.

The cross-check resulted in 2,081 instances of a voter that moved out of the state of Arizona during the 29-day period before the election who cast a ballot in the 2020 general election. It cannot be determined whether these voters undervoters all the races on their ballots other than the presidential race, thereby creating a *de facto* Presidential-Only ballot.

The ballot definitions on the Dominion EMS do not include a "Presidential-Only" ballot. The Dominion voting machines would not be able to read a ballot for which a ballot definition does not exist. Additionally, in examining the EV33 sent ballot files for ballot codes, the ballot images, and the cast vote record, no presidential-only ballots as specified by A.R.S. § 16-126 and the 2019 Election Procedures Manual were found to be cast in this election.

[20] https://www.melissa.com

NOTE: The following chart illustrates the percentage of voters by registered party that the Ballot Impacted number represents. This should give a rough idea on the impact to the electorate if the votes were cast by the voters and not another individual that was somehow able to cast a vote.

Party	%
Republican Party	41.28%
Democrat Party	31.57%
Prefer Not to Declare	21.96%
Independent	4.32%
Libertarian Party	0.82%
Green Party	0.05%

NOTE: Please see Appendix H1 for details on the voters who moved out-of-state during the 29-day period preceding the election.

5.5.4.1 References

- Arizona State - 2019 Elections Procedure Manual[21]
- A.R.S. § 16-126 – Authority to vote in a presidential election after moving from state[22]
- A.R.S. § 16-103 – Qualified person temporarily absent from the state[23]

5.5.4.2 Data Files Utilized

File Name	MD5 Hash
Maricopa County-VM55 Final Voted Nov2020 PBRQ	43070bc7afdf40a37cd45092e9733654

5.5.4.3 Recommendation

Legislation should be considered that links voter roll registration to changes in driver's licenses or other state identification, as well as requiring the current voter rolls be validated against the United States Postal Service (USPS) National Change of Address (NCOA) at a predefined period prior to every election.

Laws already exist for interstate reporting of changes in residence, addresses, and driver's licenses. Tying voter roll registration to these forms of identification would greatly increase the likelihood that voter registration details would be kept up to date. Individuals are more likely to remember their license needs to be updated immediately than voter registration, and since most states now offer the ability to register to vote when getting a license, license updates could also update voter rolls.

It is recommended that the voter rolls be validated against the NCOA both 90 days or more prior to the election, in addition to a week before mail-in ballots are sent out. This check would be utilized to determine if a mail-in ballot would be sent to the address since ballots are not allowed to be forwarded. The legislature may want to consider whether a change of address should suspend Permanent Early Voting List (PEVL) enrollment.

[21] https://azsos.gov/sites/default/files/2019_ELECTIONS_PROCEDURES_MANUAL_APPROVED.pdf
[22] https://www.azleg.gov/ars/16/00126.htm
[23] https://www.azleg.gov/ars/16/00103.htm

5.5.5 Votes Counted in Excess of Voters Who Voted

Ballots Impacted 1551

The number of votes cast in an election should not exceed the number of voters who participate in the election. An analysis of the Maricopa County Official Canvass and the VM55 Final Voted file from November 2020 show that multiple precincts counted votes in excess of the number of voters who participated in the 2020 General Election.

Reconciliation of the voters who participated to ballots cast is first required at a every vote center for election day voting. The County Audit Board is required to reconcile the voters who participated with the ballots cast for each precinct prior to certifying the Official Canvass. The expected delta should be more voters who voted than votes cast because some ballots were undervoted or overvoted. There were 277 precincts with a voter deficit, 65 precincts with an equal number of voters who voted, and cards cast. There were 401 precincts with the expected surplus.

NOTE: We've been informed shortly before the release of this report that some of the discrepancies outlined could be due to the protected voter list. This has not been able to be validated at this time, but we thought it was important to disclose this information for accuracy.

NOTE: The following chart illustrates the percentage of voters by registered party that are given within the precincts that the Ballot Impacted number represents. Understanding why there is more votes than voters in this precinct would be required before any determination could be made as to whether the precinct breakouts would influence how this finding impacted the votes.

Party	%
Republican Party	42.25%
Democrat Party	30.02%
Prefer Not to Declare	22.34%
Independent	4.41%
Libertarian Party	0.90%
Green Party	0.0%

From the Arizona Election Procedure Manual, the Audit Board has several responsibilities:

"1. Receives the Official Ballot Reports for each voting location and any supplemental information from the election boards that could explain any discrepancies.

2. Receives the signature rosters, poll lists (or scanned copies), or reports from e-pollbooks that show voter check-ins and signatures…"

"9. Identifies discrepancies in the reports following final tabulation of duplicated ballots and provisional ballots.

10. Resolves problems that appear to be of major significance in the presence of political party observers; and

11. Resolves and documents all discrepancies. The functions of the Audit Board must be completed prior to the acceptance of the canvassing."

Note that the Audit Board must consider discrepancies after the final tabulation which would include discrepancies in the number of votes counted vs. the number of voters who participated in the election. This would include mail ballots, duplicated ballots and provisional ballots for voters in every precinct. Maricopa County failed to resolve these discrepancies prior to acceptance of the canvass.

NOTE: Please see Appendix I1 for the full list broken out by precinct.

5.5.5.1 References

- State of Arizona – 2019 Elections Procedures Manual[24]

5.5.5.2 Data Files Utilized

File Name	MD5 Hash
11-03-2020-2b Final SOV and Official Canvass Report NOV2020.csv	e907163ef4b0d99e116c24fcb98a6969
Maricopa County-VM55 Final Voted Nov2020 PBRQ	43070bc7afdf40a37cd45092e9733654

[24] https://azsos.gov/sites/default/files/2019_ELECTIONS_PROCEDURES_MANUAL_APPROVED.pdf

6.5.5.3 Recommendation

Maricopa County Election Officials and Audit Board should examine all records and resolve all discrepancies prior to certification of election results. Each legal voter should be permitted to vote one and only one time.

5.6 Low Findings

5.6.1 Voters Not Part of the Official Precinct Register

Ballots Impacted 618

The list of individuals who are eligible and able to vote in an election, also known as the official precinct register, is established 10 days prior to the election. This means that for the 2020 General Election this was established on October 22nd. At that point in time everyone who was officially on the voter rolls for the election should have been on the rolls. It should not require an earlier or a later voter roll file to find a complete list of everyone who was eligible and actually voted in the election. However, a review of the VM55 Final Voted File for the 2020 General Election shows voter IDs that do not show on either the October 2, 2020 voter rolls or on the November 7, 2020 voter rolls. To match up all the voter IDs that show on the VM55 Final Voted File for the 2020 General Election it requires that you look back to the April 9, 2017, voter rolls to find all the IDs: in addition to also requiring the December 4, 2020, rolls. In total it takes 12 different months VM34 Monthly Voter Roll files to find and match-up all voters in the 2020 General Election. This can be seen in the diagram below.

VM34 File Date	# Of Matched Voters
12/4/2020	605
11/7/2020	2,089,465
9/5/2020	1
8/8/2020	1
7/3/2020	1
6/6/2020	1
12/6/2019	2
10/5/2019	3
4/5/2019	1
2/2/2019	1
5/6/2017	1
4/9/2017	1

NOTE: It is expected that the official precinct registration might be missing a few people who hadn't provided proof of citizenship prior, and has until 7pm on election day to provide this information; or those who qualify for UOCAVA who are allowed to register to vote up until 7pm on election day. However, in both cases you would expect these individuals to be in the November 7th rolls, which occurs after the election.

NOTE: Please see Appendix A for a copy of the VM55 Final Voted File joined to the appropriate rows of data from all of the above VM34s. This file is utilized as the basis for every finding that requires both VM55 and VM34 data.

NOTE: The following chart illustrates the percentage of voters by registered party that the Ballot Impacted number represents. This should give a rough idea on the impact to the electorate if the votes were cast by the voters and not another individual that was somehow able to cast a vote.

Party	%
Republican Party	37.06%
Democrat Party	34.79%
Prefer Not to Declare	26.54%
Libertarian Party	1.13%
Independent	0.49%

5.6.1.1 References

- A.R.S. § 16-168 - Precinct registers[25]

5.6.1.2 Data Files Utilized

File Name	MD5 Hash
Maricopa County-VM55 Final Voted Nov2020 PBRQ	43070bc7afdf40a37cd45092e9733654
Maricopa County-VM34 Voter Registration Oct 2, 2020	99a4440ae9bab7f0de96d7656b4e739d
Maricopa County-VM34 Voter Registration Nov 7, 2020	d7bfc018296832836d2bd8de440cba53
Maricopa County-VM34 Voter Registration Dec 4, 2020	255f69007b253c7f2737b050c439f269

5.6.1.3 Recommendation

Legislation should be considered that will require that the precinct registers be complete and comprehensive of every individual who could legally vote for the election.

[25] https://www.azleg.gov/ars/16/00168.htm

5.6.2 Duplicated Ballots Incorrect & Missing Serial Numbers

Ballots Impacted ~500

Damaged Ballots sent to duplication must have a serial number that can be matched to the duplicate (replacement ballot). Many damaged ballots sent to duplication do not have a serial number, and multiple duplicated ballots have incorrect serial numbers that do not match the original ballots. The County must "record an identical serial number on both the original and duplicate ballot (including spoiled duplicates) – this ties the ballots together and creates a paper trail as required by statute, A.R.S. § 16-621(A)"

In addition, there are hundreds of damaged ballots with unreadable serial numbers like these examples below:

[redacted]

Of those original ballots that had a readable serial number, several of them had incorrect serial numbers. In some cases, as shown in the example below, the audit team was able to identify the original ballot and the duplicate ballot based on a series of precinct, ballot type and presidential selection. The five ballots in the table below had incorrect serial numbers on the duplicate ballot.

Duplicate Ballot Serial Number	Precinct	Ballot Type	Presidential Selection	Original Damaged Ballot Serial Number
DUPBOARD3HAND0214	643	0	Biden	Board 1 Hand Dup 214
DUPBOARD3HAND0215	239	99	Trump	Board 1 Hand Dup 215
DUPBOARD3HAND0216	391	99	Biden	Board 1 Hand Dup 216
DUPBOARD3HAND0217	144	99	Biden	Board 1 Hand Dup 217
DUPBOARD3HAND0218	492	0	Biden	Board 1 Hand Dup 218

[redacted]

Segment Trailer Sheet showing precinct and ballot type

UOCAVA Ballot Image showing precinct, ballot type

5.6.2.1 REFERENCES

- State of Arizona – 2019 Elections Procedures Manual[26]
- A.R.S. § 16-621 – Proceedings at the counting center[27]

5.6.2.2 RECOMMENDATION

Legislation should be considered that requires regular audits of the duplicate ballot process.

[26] https://azsos.gov/sites/default/files/2019_ELECTIONS_PROCEDURES_MANUAL_APPROVED.pdf
[27] https://www.azleg.gov/ars/16/00621.htm

5.6.3 Ballots Returned Not in the Final Voted File

Ballots Impacted 430

Ballots show as returned in the EV33 Early Voting Returns File but there is no matching record in the VM55 Final Voted File. All entries in the EV33 file show with a ballot status of "Returned" and the only other status of "Voided Early Ballot" is not used anytime in the 2020 General Election.

The most likely explanation is that these ballots represent rejected ballots. However, the number of ballots in question, 2,472, does not match the 2,976 ballots that were rejected (2,042) or late (934). It is expected there should be a full accounting of all ballots received and voted that can be matched up to individual voter participation.

NOTE: Please see Appendix K1 for a list of all the EV33 entries that cannot be found in the VM55 file.

NOTE: The following chart illustrates the percentage of voters by registered party that the Ballot Impacted number represents. This should give a rough idea on the impact to the electorate if the votes were cast by the voters and not another individual that was somehow able to cast a vote.

Party	%
Republican Party	33.25%
Democrat Party	32.12%
Prefer Not to Declare	29.41%
Independent	3.84%
Libertarian Party	1.05%
Green Party	0.25%
Independent	0.08%

5.6.3.1 References

- A.R.S. 16-542 – Request for ballot[28]
- A.R.S. 16-246 – Early Balloting[29]

[28] https://www.azleg.gov/ars/16/00542.htm
[29] https://www.azleg.gov/ars/16/00246.htm

5.6.3.2 Data Files Utilized

File Name	MD5 Hash
Maricopa County-VM55 Final Voted Nov2020 PBRQ	43070bc7afdf40a37cd45092e9733654
EV33-1377-10-09-2020_101111.txt	f1daa7089f7300237f6b4ff779661cf9
EV33-1377-10-12-2020_113210.txt	72e4e6c102e3539b4dd15b4454357b69
EV33-1377-10-13-2020_111553.txt	9b14841281c031533322b50aabb86a24
EV33-1377-10-14-2020_112757.txt	1b7537d7d9b927dbf4e462ed5ee8f97c
EV33-1377-10-15-2020_121331.txt	dec7d08dde4970c26e32b8c844f4a9ab
EV33-1377-10-16-2020_113522.txt	f0a632c3fd9b5f177d48504dc119be31
EV33-1377-10-19-2020_111708.txt	db80b692a9188add0844a8974e227287
EV33-1377-10-20-2020_112351.txt	57d1795db8be71d516e29350e347fb3a
EV33-1377-10-21-2020_111843.txt	56c3b5a11651c68735164c578eade4e1
EV33-1377-10-22-2020_111714.txt	03551f170bf758efc90c013d0fe2e467
EV33-1377-10-23-2020_112614.txt	dbfdd369ac148723540c83f614cca454
EV33-1377-10-26-2020_111318.txt	0b68adff779f59c70a530000bf989aca
EV33-1377-10-27-2020_111413.txt	a6fc7377bf6c6fe6653f539c5970a6f7
EV33-1377-10-28-2020_111331.txt	43758b9290f90d0305d5ed84aa10becb
EV33-1377-10-29-2020_111300.txt	410b30b06f2ca73022f27173fe114038
EV33-1377-10-30-2020_111804.txt	5cb44e5ea214f40227e04345d4355ff7
EV33-1377-11-02-2020_111214.txt	5d15bb8686a022f53400550cfe010a07

5.6.3.3 Recommendation

Legislation should be considered that requires that the various election related systems to properly integrate in order to give accurate and consistent counts between the mail-in ballots cast, mail-in ballots received, mail-in ballots accepted, mail-in ballots rejected, and be able to reconcile these details with who voted in the final voted file.

5.6.4 Mail-In Ballot Received Without Record of Being Sent

Ballots Impacted 397

Ballots show as returned in the EV33 Early Voting Returns File for a voter who voted by mail but there is no matching record in the EV32 Early Voting Sent File showing that a ballot was ever sent. This most likely means that there was a clerical error in the EV32 Early Voting Sent Files and ballots that were sent out legitimately were not recorded.

NOTE: At an earlier hearing it was stated that there were 74,243 entries in EV33 Early Voting Returns Files without a corresponding entry in the EV32 Early Voting Sent Files. This was brought up in the context of justification for performing canvassing to further validate the reasoning for this discrepancy. While this discrepancy is accurate, it was unintentionally misleading. All but 397 of those entries were Early Voting in-person votes which also generate an EV33 entry in addition to mail-in ballots.

NOTE: The following chart illustrates the percentage of voters by registered party that the Ballot Impacted number represents. This should give a rough idea on the impact to the electorate if the votes were cast by the voters and not another individual that was somehow able to cast a vote.

Party	%
Democrat Party	33.25%
Republican Party	31.49%
Prefer Not to Declare	29.72%
Independent	3.53%
Libertarian Party	2.02%
Green Party	0.08%

NOTE: Please see Appendix L1 for a complete list of the voters who had a ballot received, but there is no record of a ballot being sent.

5.6.4.1 References

- A.R.S. 16-542 – Request for ballot[30]
- A.R.S. 16-246 – Early Balloting[31]

5.6.4.2 Data Files Utilized

File Name	MD5 Hash
Maricopa County-VM55 Final Voted Nov2020 PBRQ	43070bc7afdf40a37cd45092e9733654
EV33-1377-10-09-2020_101111.txt	f1daa7089f7300237f6b4ff779661cf9
EV33-1377-10-12-2020_113210.txt	72e4e6c102e3539b4dd15b4454357b69
EV33-1377-10-13-2020_111553.txt	9b14841281c031533322b50aabb86a24
EV33-1377-10-14-2020_112757.txt	1b7537d7d9b927dbf4e462ed5ee8f97c
EV33-1377-10-15-2020_121331.txt	dec7d08dde4970c26e32b8c844f4a9ab
EV33-1377-10-16-2020_113522.txt	f0a632c3fd9b5f177d48504dc119be31
EV33-1377-10-19-2020_111708.txt	db80b692a9188add0844a8974e227287
EV33-1377-10-20-2020_112351.txt	57d1795db8be71d516e29350e347fb3a
EV33-1377-10-21-2020_111843.txt	56c3b5a11651c68735164c578eade4e1
EV33-1377-10-22-2020_111714.txt	03551f170bf758efc90c013d0fe2e467
EV33-1377-10-23-2020_112614.txt	dbfdd369ac148723540c83f614cca454
EV33-1377-10-26-2020_111318.txt	0b68adff779f59c70a530000bf989aca
EV33-1377-10-27-2020_111413.txt	a6fc7377bf6c6fe6653f539c5970a6f7
EV33-1377-10-28-2020_111331.txt	43758b9290f90d0305d5ed84aa10becb
EV33-1377-10-29-2020_111300.txt	410b30b06f2ca73022f27173fe114038
EV33-1377-10-30-2020_111804.txt	5cb44e5ea214f40227e04345d4355ff7
EV33-1377-11-02-2020_111214.txt	5d15bb8686a022f53400550cfe010a07
EV32-1377-09-18-2020_075112.txt	ab22e9ba4ad54af1b7a47f8381d506c7
EV32-1377-09-30-2020_111728.txt	2e4df9ccf2e5e64fd7e164628ff7667a

[30] https://www.azleg.gov/ars/16/00168.htm
[31] https://www.azleg.gov/ars/16/00246.htm

File Name	MD5 Hash
EV32-1377-10-01-2020_113125.txt	92538fe838c7c872957d155a98290874
EV32-1377-10-02-2020_125658.txt	be7d44838daa2aa758a0adb1dfe88acd
EV32-1377-10-05-2020_112338.txt	31a356a1a1826639759fc66afb812498
EV32-1377-10-06-2020_114600.txt	cb70c4468ebd51142003e46e3e1257c4
EV32-1377-10-07-2020_111951.txt	185d423606927ba15f827e19329c02aa
EV32-1377-10-08-2020_111639.txt	4f82598b6fab071300e92b8f56407451
EV32-1377-10-09-2020_112718.txt	bdf22cce7eca5eeb0b52dbb9f87a54b6
EV32-1377-10-12-2020_113153.txt	67a7ab52ab0850127528b18667eaf5c6
EV32-1377-10-13-2020_111535.txt	81af1c0b010368d0e11cc68e8a21f2e6
EV32-1377-10-14-2020_112738.txt	e88cce6a8a27b5bf755765f516710c48
EV32-1377-10-15-2020_121305.txt	2f12b801d981afc0e4e114bdfbf4241c
EV32-1377-10-16-2020_113410.txt	46a251f88fdd1d2e2352ac1dc61fffa9
Maricopa_EV32-1377-10-19-2020_111633-2020-10-20T14 53 30Z.txt	9cd6e80c07e1f33129cf98302930abb6
Maricopa_EV32-1377-10-20-2020_112309-2020-10-21T15 13 12Z.txt	e3cc25b520b5710090f4dfff2d7fce7f
Maricopa_EV32-1377-10-21-2020_111759-2020-10-22T15 08 54Z.txt	e786fec02788d0b7c4392ca5b1cd284e
Maricopa_EV32-1377-10-22-2020_111639-2020-10-23T15 03 40Z.txt	86ea315f6bce7c0c902027b5373f6e2c
Maricopa_EV32-1377-10-23-2020_112532-2020-10-26T15 00 59Z.txt	ca42553da16ea38cf2b72f29b81a990f

5.6.4.3 Recommendation

It is recommended that the Attorney General inquire of Maricopa County as to the reason for this discrepancy, and if a sufficient explanation is not received an investigation be opened to investigate this further.

5.6.5 Voters With Incomplete Names

Ballots Impacted 393

A.R.S. 16-152 requires that the form used for the registration of electors shall contain the registrant's given name, middle name, if any, and surname.

The 11/07/2020 VM34 contains 720 voters with incomplete names. 393 of these voters voted in the 2020 General Election.

Examples of incomplete names include:

- Voters with only a last name
- Voters with only an initial for their last name
- Voters with an initial for their first name and last name
- Voters with no last name
- Voters with only an initial for their first name

NOTE: It is possible to have a legal name that is just an initial, or to not have a surname. However, this is extremely rare, and the list should be reviewed to determine its accuracy.

Description	Number of voters
Last name only	15
Last name is an initial only	9
No last name	45
First name is an initial only	324
Total	**393**

The 2019 Elections Procedure Manual addresses failure to provide name. "If the State Form, Federal Form, FPCA, or FWAB does not contain the registrant's name, residence address or location, DOB, or signature (or assisting person's signature), but the County Recorder has the address, telephone number, or email address to contact the registrant to request the incomplete information, the registrant should be entered into the voter registration database in a "suspense" status until the incomplete information or a new voter registration form is received. A.R.S. § 16-134(B); A.R.S. § 16-121.01(A)." (pgs. 18-19)

If the registrant does not provide the missing, incomplete, or illegible information by 7:00 p.m. on the date of the next regular general election, the registration form is invalid and the registrant's status may be changed from "suspense" to "not registered," with the reason code "pending expired" (or functional equivalent). The registrant would need to submit a new voter registration application to be eligible to vote in future elections. (pg. 19)

NOTE: The following chart illustrates the percentage of voters by registered party that the Ballot Impacted number represents. This should give a rough idea on the impact to the electorate if the votes were cast by the voters and not another individual that was somehow able to cast a vote.

Party	%
Democrat Party	34.35%
Republican Party	32.57%
Prefer Not to Declare	24.43%
Independent	6.87%
Libertarian Party	1.27%
Green Party	.51%

NOTE: Please see Appendixes M1 and M2 for a list of voters with incomplete names who voted, and a list of all incomplete names on the November 7, 2020 voter rolls.

5.6.5.1 References

- A.R.S. 16-152 – Registration Form[32]
- State of Arizona - 2019 Elections Procedure Manual[33]

5.6.5.2 Data Files Utilized

File Name	MD5 Hash
Maricopa County-VM55 Final Voted Nov2020 PBRQ	43070bc7afdf40a37cd45092e9733654

5.6.5.3 Recommendation

Legislation should be considered that requires the voter registration entries be a direct match with any acceptable form of government identification, and always checked against that identification to validate compliance. If existing laws are sufficient that this should be occurring, additional legislation should be considered to increase the likelihood of compliance such as penalties.

5.6.6 Deceased Voters

Ballots Impacted 282

The Final Voted File, or VM55, was cross-checked against a commercially available data source provided by Melissa[34] called Personator, and it was found that 282 individuals who were flagged as deceased prior to October 5, 2020, voted in the election.

Personator is a best-in-class identity and address validation tool. It confirms that an individual is associated with an address, indicates prior and current addresses, tracks when and where the individual moves, tracks date-of-birth and date-of-death. To accomplish this, it utilized both private and government data sources such as the US Postal Service's National Change of Address (NCOA) service, and the Social Security Administration's Master Death List.

NOTE: It is recommended that the Attorney General further investigate this finding to confirm the validity of this finding, and if applicable, determine who cast the vote on behalf of the deceased individual.

[32] https://www.azleg.gov/ars/16/00152.htm
[33] https://azsos.gov/sites/default/files/2019_ELECTIONS_PROCEDURES_MANUAL_APPROVED.pdf
[34] https://www.melissa.com

NOTE: The following chart illustrates the percentage of voters by registered party that the Ballot Impacted number represents. This should give a rough idea on the impact to the electorate if the votes were cast by the voters and not another individual that was somehow able to cast a vote.

Party	%
Republican Party	49.65%
Democrat Party	30.14%
Prefer Not to Declare	12.77%
Independent	7.09%
Libertarian Party	0.35%

NOTE: Please see Appendix N1 for a complete list of individuals who show as being dead in Melissa.

5.6.6.1 Data Files Utilized

File Name	MD5 Hash
Maricopa County-VM55 Final Voted Nov2020 PBRQ	43070bc7afdf40a37cd45092e9733654

5.6.6.2 Recommendation

Legislation should be considered to require the voter rolls to periodically be compared against the Social Security's Master Death List, or other commercially available tools that gives access to this information. A minimum frequency on to conduct this should specifically be required.

5.6.7 Audit UOCAVA Count Does Not Match the EAC Count

Ballots Impacted 226

The Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) requires all counties in the United States to report data related to the ability of civilian, military, and overseas citizens to register to vote and successfully cast a ballot. Analysis of the data submitted by Maricopa to the US Election Commission shows discrepancies in the number of ballots reported by the County to the EAC and the number of ballots observed during the audit. The audit team found 226 more electronically submitted UOCAVA ballots than the County reported to the EAC. Any UOCAVA ballots returned by mail were not identified as UOCAVA. Therefore, the audit team used the County mail numbers reported to the EAC. A Public Records Request for UOCAVA data was submitted to the Arizona Secretary of State but as of this date, no records have been provided in response to that request.

Election Administration Voting Survey 2020 vs Audit Counts

UOCAVA Type	EAVS 2020	Audit Count	Discrepancy
Electronically	8,988	9,214	-226
Mail	1,420	Comingled	Unknown
Total	10,408	-	-

While many people believe that UOCAVA is a law that primarily enables active-duty military men and women to vote, it is used more often by non-military voters. See below table of the total number of Civilian vs Military voters who were UOCAVA eligible in Maricopa County based on the November 07, 2020, VM34 Monthly Voter Rolls.

Military Returned Ballots	Military % of UOCAVA	Civilian Ballots Returned	Civilian % of UOCAVA
4,359	35%	7,934	65%

The law allows military voters who are out of their home county to vote electronically. However, non-military voters (civilians) who are not out of the country are not eligible to vote electronically. According to Maricopa County's UOCAVA Map website, more than 140 civilians – who were not UOCAVA eligible due to being in the United States--were permitted to vote via UOCAVA in the 2020 General Election.

The Uniformed and Overseas Citizens Absentee Voting Act defines eligibility as:

- A member of a uniformed service on active duty who, by reason of such active duty, is absent from the place of residence where the member is otherwise qualified to vote;
- A member of the merchant marines who, by reason of service in the merchant marine, is absent from the place of residence where the member is otherwise qualified to vote; or
- A spouse or dependent of a member referred to above who, by reason of the active duty or service of the member, is absent from the place of residence where the spouse or dependent is otherwise qualified to vote.
- An absent uniformed services voter who, by reason of active duty or service is absent from the United States on the date of the election involved;
- A person who resides outside the United States and is qualified to vote in the last place in which the person was domiciled before leaving the United States; or
- A person who resides outside the United States and (but for such residence) would be qualified to vote in the last place in which the person was domiciled before leaving the United States

Maricopa County shows that there are 12,293 eligible UOCAVA voters based on the November 7, 2020, VM34 Monthly Voter Rolls. Of these UOCAVA ballots transmitted, 85% or 10,408 were reported as returned. Historically, approximately 68% of UOCAVA voters return their ballot.

5.6.7.1 References

- State of Arizona – 2019 Elections Procedures Manual[35]
- Maricopa County UOCAVA Map Website[36]
- US Election Commission 2020 Survey Results[37]
- US Election Commission 2016 Survey Results[38]

[35] https://azsos.gov/sites/default/files/2019_ELECTIONS_PROCEDURES_MANUAL_APPROVED.pdf
[36] https://recorder.maricopa.gov/uocavamap/
[37] https://www.eac.gov/research-and-data/studies-and-reports
[38] https://www.eac.gov/sites/default/files/eac_assets/1/6/2016_EAVS_Comprehensive_Report.pdf

5.6.7.2 Data Files Utilized

File Name	MD5 Hash
11-03-2020-0 Canvass COMPLETE NOV2020	ce62cc061b6bb56b4fd40aa4866adb16
Maricopa County-VM34 Voter Registration Nov 7, 2020	d7bfc018296832836d2bd8de440cba53

5.6.7.3 Recommendation

Legislators should consider auditing the UOCAVA voting system to determine whether any changes are required to ensure the integrity of the vote.

5.6.8 Late Registered Voters with Counted Votes

Ballots Impacted 198

Individuals who registered to vote after the October 15th deadline were allowed to cast a vote and these votes were counted. The Final Voted File, or the VM55, is the official record of who cast a vote for a given election. This file does not contain the Date of Registration for individuals who voted in the election, but it does include each person's Voter ID which can be cross referenced against the Full Voter File, or VM34, to get the registration date value.

It would be expected that either the October or the November VM34 file would contain all of the registered voters that voted in on the November 2020 General Election, but this was not the case. It took 12 different VM34 files ranging from April 9, 2017, to December 4th, 2020, to find all of the Voter IDs found in the Final Voted VM55 File for the 2020 General Election.

When utilizing multiple Full Voter Files that span multiple years it can get complicated to determine which data for a given Voter ID should be utilized when that Voter ID is found in more than one file. For the purpose of our analysis for this and other findings we assumed that the November 7, 2020, VM34 file would be the most accurate since it was right after the election, and the only VM34 officially provided by Maricopa County as part of a subpoena.

As a result, we loaded the data from VM34 files for every month from January 2017 through December 2020 into a database. First, we loaded the December 4, 2020, VM34 file. We then subsequently loaded the VM34 files from the oldest to the newest, with each subsequent VM34 file replacing the stored data for any Voter ID that had existed in a prior load and finishing with the November 7, 2020, file. This ensured that we always had the most current data for a given Voter ID, and the latest data from the last time a given Voter ID showed up in a VM34 file would always be utilized.

This composite VM34 file was then matched up with the VM55 file to provide additional details for all voters within the Final Voted VM55 file.

In all, it required data from the following VM34 files to match all the data:

VM34 File Date	# Of Matched Voters
12/4/2020	605
11/7/2020	2,089,465
9/5/2020	1
8/8/2020	1
7/3/2020	1
6/6/2020	1
12/6/2019	2
10/5/2019	3
4/5/2019	1
2/2/2019	1
5/6/2017	1
4/9/2017	1

When building this file in this manner there were 198 voters registered after October 15th who voted in the election and had their vote counted, according to the Final Voted File.

NOTE: Individuals who register according to the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) were not included in this list as the rules for UOCAVA allow registration up to 7:00pm on election day.

NOTE: Publicly, we had stated that there were 3,981 individuals who had registered after October 15th and voted. This was based on a wrong assumption by one of our data analysts who concluded that the only way the Official Canvass could match the Final Voted VM55 file was if those voters flagged as "Q," or uncounted provisional ballots, were in fact counted in the Official Canvass. While the discrepancy between the Official Canvass and the VM55 numbers are very similar to that number, assumptions should not have been made as to the reasoning for that.

NOTE: The following chart illustrates the percentage of voters by registered party that the Ballot Impacted number represents. This should give a rough idea on the impact to the electorate if the votes were cast by the voters and not another individual that was somehow able to cast a vote.

Party	%
Republican Party	33.84%
Democrat Party	31.82%
Prefer Not to Declare	33.33%
Independent	0.51%
Libertarian Party	0.51%

NOTE: Please see Appendix A for the complete VM55 Final Voted File with all of the various VM34 files.

NOTE: Please see Appendix O1 for a list of the late registered voters who voted.

5.6.8.1 References

- A.R.S. § 16-152 – Registration Form[39]
- A.R.S. § 16-120 – Eligibility to vote[40]
- A.R.S. § 16-101 – Qualifications of registrant[41]

5.6.8.2 Data Files Utilized

File Name	MD5 Hash
Maricopa County-VM55 Final Voted Nov2020 PBRQ	43070bc7afdf40a37cd45092e9733654
Maricopa County-VM34 Voter Registration Oct 2, 2020	99a4440ae9bab7f0de96d7656b4e739d
Maricopa County-VM34 Voter Registration Nov 7, 2020	d7bfc018296832836d2bd8de440cba53
Maricopa County-VM34 Voter Registration Dec 4, 2020	255f69007b253c7f2737b050c439f269

5.6.8.3 Recommendation

Legislation should be considered that would require applications developed and utilized for voter rolls or voting to be developed to rigorous standards that ensure the confidentiality and integrity of the systems. This would prevent the entry of invalid data. Specifically, its recommended that the Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS) Level 3 be applied to all applications associated with voter rolls or voting and that it be required that this be fully validated no less than once every two years.

5.6.9 Date of Registration Changes to Earlier Date

Ballots Impacted 193

Dates of Registration in the Full Voter File, also known as a VM34, are periodically changing, including changing to earlier dates. Dates of Registration are significant because they can determine if someone is eligible to vote in an election, or if they're not eligible. Based on communications with the Maricopa County Recorder's Office, Dates of Registration should never change except for fixing the occasional mistake.

A review of the November 7, 2020, VM34 file and subsequent VM34 files for the remainder of 2020 and into 2021 show 891 dates of registration changes that would have made someone eligible to vote in the November 2020 General Election when their date of registration shown on the November 7th file would have prohibited it. Out of these 890 dates of registration, 193 had their votes counted in the 2020 General Election despite still having an ineligible date of registration on the November 7th VM34.

[39] https://www.azleg.gov/ars/16/00152.htm
[40] https://www.azleg.gov/ars/16/00120.htm
[41] https://www.azleg.gov/ars/16/00101.htm

NOTE: The following chart illustrates the percentage of voters by registered party that the Ballot Impacted number represents. This should give a rough idea on the impact to the electorate if the votes were cast by the voters and not another individual that was somehow able to cast a vote.

Party	%
Prefer Not to Declare	34.20%
Republican Party	33.16%
Democrat Party	31.61%
Independent	0.52%
Libertarian Party	0.52%

NOTE: Please see Appendix P1 for more details on the voters whose registration dates were changed to an earlier date.

----- Forwarded Message -----
From: voterinfo - RISCX <voterinfo@risc.maricopa.gov>
To: [redacted]
Sent: Friday, September 3, 2021, 04:51:57 PM MST
Subject: RE: Customer Website Comments - Voter Information

Hello [redacted]

Thank you for your questions.

Are there any circumstances in which someone's registration date can change?

Generally, a voter's date of registration does not change outside of correcting a mistake. The date of registration is the date where the voter first registered to vote in in the county, while any updates to a voter's registration is tracked separately.

The only time a voter may have two dates of registration is if their registration has previously been cancelled and the voter registers again. The original record could be cancelled for a variety of reasons, including death of the voter, voter request, or the voter has moved outside Maricopa County. Only the latest voter registration record is considered valid and a voter cannot use their cancelled record.

Does it always reflect the original registration in Maricopa County or can someone transfer a registration from another county?

The date of registration will always reflect the original date of registration in the county where the voter lives. Voter rolls are maintained at the county level, so counties only keep records of the voters in their jurisdiction. For example, Maricopa County can process and access records for our 2.6 million voters, but we do not keep records of Pima County voters.

If a voter moves to another county or state, that voter will have to reregister in their new location. We cannot transfer a voter registration between counties or states.

5.6.9.1 References

- A.R.S. § 16-152 – Registration Form[42]
- A.R.S. § 16-120 – Eligibility to vote[43]
- A.R.S. § 16-101 – Qualifications of registrant[44]

5.6.9.2 Data Files Utilized

File Name	MD5 Hash
Maricopa County-VM55 Final Voted Nov2020 PBRQ	43070bc7afdf40a37cd45092e9733654
Maricopa County-VM34 Voter Registration Oct 2, 2020	99a4440ae9bab7f0de96d7656b4e739d
Maricopa County-VM34 Voter Registration Nov 7, 2020	d7bfc018296832836d2bd8de440cba53
Maricopa County-VM34 Voter Registration Dec 4, 2020	255f69007b253c7f2737b050c439f269

5.6.9.3 Recommendation

Legislation should be considered that would require applications developed and utilized for voter rolls or voting to be developed to rigorous standards that ensure the confidentiality and integrity of the systems. Specifically, its recommended that the Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS) Level 3 be applied to all applications associated with voter rolls or voting and that it be required that this be fully validated no less than once every two years.

[42] https://www.azleg.gov/ars/16/00152.htm
[43] https://www.azleg.gov/ars/16/00120.htm
[44] https://www.azleg.gov/ars/16/00101.htm

5.6.10 Duplicate Voter IDs

Ballots Impacted 186

Individuals were found within the voter rolls that had the same first name, last name, shared an address at one point in the past, and their birth years were within 10 years; suggesting they're the same person, but multiple Voter IDs. In all 186 cases both VoterIDs voted in the 2020 General Election.

NOTE: All Voter ID's associated with this finding can be found in Appendix Q1. This finding is not any clear indication of wrongdoing, and if wrongdoing occurred it may or may not have been the result of the individual whose Voter ID is listed in this report. It is recommended that the Attorney General follow-up further and determine if any additional action is needed.

NOTE: The following chart illustrates the percentage of voters by registered party that the Ballot Impacted number represents. This should give a rough idea on the impact to the electorate if the votes were cast by the voters and not another individual that was somehow able to cast a vote.

Party	%
Democrat Party	46.15%
Republican Party	30.77%
Prefer Not to Declare	15.93%
Independent	5.49%
Libertarian Party	1.65%

5.6.10.1 Data Files Utilized

File Name	MD5 Hash
Maricopa County-VM55 Final Voted Nov2020 PBRQ	43070bc7afdf40a37cd45092e9733654
Maricopa County-VM34 Voter Registration Nov 7, 2020	d7bfc018296832836d2bd8de440cba53

5.6.10.2 Recommendation

Legislation should be considered that requires the periodic review of the voter rolls for duplicate entries by the same name and year of birth. Legislation should also be considered that would require voter registration to validate that no other registered voter on the rolls registered with the same valid identification. This would prevent both accidental and purposeful multiple registrations.

5.6.11 Multiple Voters Vinked by AFFSEQ

Ballots Impacted 101

Each voter registration form has a unique, preprinted number on it much like a serial number on paper currency. This number is called an affidavit sequence number or AFFSEQ. It is preprinted, usually in the upper right-hand corner of every registration document. Each unique AFFSEQ number represents the specific registration document it is preprinted on.

Below is an example of an actual AFFSEQ number preprinted on a voter registration document. This specific AFFSEQ number [redacted] should only ever be associated with the voter and voter ID that filled out and signed this registration form this number was printed on.

[redacted]

The County uses AFFSEQ numbers and their corresponding registration documents to record any changes or updates to an individual voter's registration record. Every time a voter fills out a registration document, whether it be to register for the first time or to update their registration information with an address change, party change or signature update, the AFFSEQ number preprinted on their form is recorded in their voter record along with the date the form was signed by the registrant. A digital image of each registration document is created. The image is titled with the AFFSEQ number of the document it represents. The AFFSEQ identifier number is unique to each transaction, unique to the voter, and should never be repeated. As with paper currency, if more than one bill is found with the same serial number, then the bills are examined to determine which bill is the original and which is the duplicate.

Comparing the VM55 Final Voted file to the Maricopa County monthly VM34 files across time, between January 6, 2018-June 6, 2021, resulted in 5,711 instances where an affidavit sequence number was shared by multiple voters. It was confirmed with the County that AFFSEQ numbers are unique to the voter and should never be repeated.

On Aug 30, 2021, at 11:52 AM, voterinfo - RISCX <voterinfo@risc.maricopa.gov> wrote:

Good morning [redacted]. The AFFSEQs refers to Affidavit sequence. Each transaction by a voter will result in an affidavit. The affidavit could be a modification to your registration such as address change, party change or an updated signature as an example. An affidavit identifier is also applied to the affidavit envelope, or a provisional ballot used during an election. These identifiers are unique to each transition and never repeated.

Thank you for your questions.

[redacted]

OFFICE OF MARICOPA COUNTY RECORDER
111 S. 3RD Ave, Ste. 103, Phoenix, AZ 85003
(602) 506-2543 Email: voterinfo@risc.maricopa.gov

Of the 5,711 instances of AFFSEQ numbers shared by multiple 2020 General Election voters, at least one vote was cast.

- In 101 of these instances, BOTH voter IDs linked by AFFSEQ voted in 2020 General Election.

160,223 AFFSEQ images were provided which is an extremely small percentage of the total AFFSEQ images that are recorded over time.

Upon examining hundreds of these AFFSEQ registration document images of voters sharing the same AFFSEQ number, it was found that:

- The same person is being assigned more than one voter ID number.
- Voter identities and their voter ID are being associated with other individuals with different names, addresses, identifying information and even of the opposite gender

The registration document images of all shared AFFSEQ numbers need to be examined to determine which associated voter is correctly associated with the document.

Three samples of the types of issues we found in the 5,711 instances are documented below.

Same Person with Two Different Voter ID's Linked by AFFSEQ-Both Voter IDs Voted in GE2020:

In this sample instance, the same person, with her name misspelled in the voter registration database, shares an AFFSEQ with herself and also has two voter IDs. In the images below you can that the same person filled out two registration forms 10 days apart, she was given a unique voter ID in each instance even though both forms were filled out with the same name, address, birth date and phone number. A vote was cast by mail-in ballot for both voter IDs.

VOTER ID	Name	Address	DOB Year	Date of Registration	VM 34 File Name	Initial AFFSEQ	Initial Change Effective Date	Linked AFFSEQ	VM55 BALTYPE
[redacted]									

Same Person with the Secondary Voter ID Given a Different Name and Address-Both Voter IDs Voted GE2020:

The first image below shows the voter information for two voters that share the same AFFSEQ number, County records show that in the 1/6/2018 VM34 file that shared the same AFFSEQ number with . These two voters have different names, addresses, and birth years.

In the registration image below, you can see that J Lancaster filled out a registration form on 4/10/2018. The preprinted AFFSEQ number on the form was . lists his birthyear as 1978 on this form. It is listed as 1975 in his voter record. He included his driver's license number as identifying information. On this form in the lower right-hand corner, a county employee wrote the voter ID number , identifying the connection with that voter ID. In row 1 of the voter record below, you see that voter ID number belongs to , not . The County employee identified that J Lancaster was connected with in some way. The date the County employee stamped this form is April 23, 2018. Both voter IDs were used to vote in the 2020 General Election.

In row 2 you can see that J Lancaster has a voter ID number of . address in the VM34 record is in Phoenix. This corresponds with his voter registration form below.

VOTER ID	Name	Address	Birth Year	Date of Registration	VM34 File Date	Initial AFFSEQ	Initial Change Effective Date	Linked AFFSEQ	VM55 BALTYPE

Male Voter Filled Out Regsitration Form but a Female is Recorded as Associated with His Registration Form, Both Are Linked by AFFSEQ-Both Voter IDs Voted GE2020:

Just as no two voters should share an AFFSEQ number, no two voters should share a voter ID number. The County confirmed that voter IDs are generated automatically and that they are never reused. It was found that not only are two voters sharing an AFFSEQ number, but they are also sharing a voter ID number.

registered to vote on 9/25/2018. The AFFSEQ on his registration form is . He was given voter ID number of In row 1 below you can see that his voter ID number is now associated with , a female, at a different address in Phoenix. This unknown person who is using original voter ID voted in the 2020 General Election using a mail in ballot. voted in person on election day.

filled out a registration form again on . He was given voter ID number . voted in 2020 General Election in person at the polls. We do not have an image of this voter registration as it was not in the limited AFFSEQ images supplied to us by the County.

VOTER ID	Name	Address	Birth Year	Date of Registration	VM34 File Date	Initial AFFSEQ	Initial Change Effective Date	Linked AFFSEQ	VM55 BALTYPE
[redacted]									

[redacted]

NOTE: The following chart illustrates the percentage of voters by registered party that the Ballot Impacted number represents. This should give a rough idea on the impact to the electorate if the votes were cast by the voters and not another individual that was somehow able to cast a vote.

Party	%
Democrat Party	42%
Republican Party	33%
Prefer Not to Declare	22%
Independent	2%
Libertarian Party	1%

NOTE: Please see Appendix R1 for a complete list of users who have shared an AFFSEQ.

5.6.11.1 References

- State of Arizona – 2019 Elections Procedures Manual[45]

5.6.11.2 Data Files Utilized

File Name	MD5 Hash
Maricopa County-VM55 Final Voted Nov2020 PBRQ	43070bc7afdf40a37cd45092e9733654
VM34_20170107_113131.txt	fb675c6b6ad9757759a1e686ce87a17f
VM34_20170204_104417.txt	02a1003bf8ddc1a0cc547032c73505db
VM34_20170305_102136.txt	708ea30d01595f1552892a13e1c11eeb
VM34_20170409_044850.txt	9b25f73a824589bd70e20fe02cb1f703
VM34_20170506_094005.txt	d8bbaacbaffba5321ac4b22d7aaebf5e
VM34_20170604_014543.txt	ecb6f6760b313b135c6a9ba7e4d6369a
VM34_20170708_091800.txt	76c897e712aba76072dff3fb68e8d29c
VM34_20170805_111659.txt	ad9f1e228123d67c9774d5c4de3a4442
VM34_20170903_031323.txt	05cfd1aa1f82392f99c65e394d526470
VM34_20171008_021223.txt	6e199b2b3fc9a98c78d4c3ee76727720
VM34_20171103_103144.txt	c7890363fbaf1de622af2f589d0a48d4
VM34_20171203_070930.txt	b796c93976f7d89cd53d09a26406fcaf
VM34_20180106_024335.txt	74823063c6c04beb0ae2ba94789992b8
VM34_20180203_063848.txt	6b55c00202aa4edb39bb47bac27e7545
VM34_20180302_095453.txt	8c6e9e7edaaff58b2b4635c3ad56369c
VM34_20180406_081509.txt	fc3f8d71d9cdfebc10aeaf7fb5c4290b
VM34_20180504_093125.txt	fa683fa02fd0d9bfcbc52a106af6873e
VM34_20180602_102915.txt	c99fd11d76648af61948842161d1d197
VM34_20180707_024237.txt	b6141774c149ea2f7695e230d5f78eb9
VM34_20180803_115351.txt	351a3107ef1a7e5a907c1137393216ee
VM34_20180907_091404.txt	62e7d11db59dbb5be078b7a3374125be
VM34_20181005_112120.txt	1b07988566c762821d625a0477269d3c
VM34_20181102_105026.txt	cb73855d70509a13a52beedde18666a3
VM34_20181209_032523.txt	9838a26c37f016d0e87adb43a9501707
VM34_20190106_084008.txt	6f4be0c41404d12bb0f6ff69d8f27a28
VM34_20190202_063949.txt	cc8a7b9b1cf66a9b8fce0905df71af74
VM34_20190302_090830.txt	15ec5c127b37ec91c1c14708e7a9421d
VM34_20190405_074946.txt	fb6ecbf069154cbb8149d4af8348c6c4
VM34_20190503_080954.txt	b130edae7a4ae04afcf8e459c085fc2d
VM34_20190608_035533.txt	301287923fc8327b259c286712f0b38c
VM34_20190705_102047.txt	b89551ec6616a148a0a6eb0d9a9eb9a4
VM34_20190802_093213.txt	b2517193b03f9820c3588789890cd505
VM34_20190906_115511.txt	7fe4f70c92e995a87cd67c69feac348a
VM34_20191005_075436.txt	30cd819a5b53759ebd9b35fcf4f2f515

[45] https://azsos.gov/sites/default/files/2019_ELECTIONS_PROCEDURES_MANUAL_APPROVED.pdf

File Name	MD5 Hash
VM34_20191206_062132.txt	4d7d56540c50bcb9efd53882f65dafa9
VM34ALL_20201107_003451.txt	d7bfc018296832836d2bd8de440cba53
VM34_20200103_062658.txt	ea5eb36acb1f3a20204fc860578755bc
VM34_20200208_124009.txt	cb840187d01b8d26f4a192a29de0729a
VM34_20200306_114048.txt	92b41e30958182e994ff86b5600c9002
VM34_20200403_113114.txt	5460b45b91f6709ee118e2385020b102
VM34_20200502_014453.txt	c44bf7968e9bf4fde446f5c43da584ef
VM34_20200606_001100.txt	1d8b12eea610b5b55f07d9fad1d8af80
VM34_20200703_213734.txt	47afb6e874c859a08c4105f912981330
VM34_20200808_004341.txt	8cb279714659f945f154129ea757f677
VM34_20200905_001156.txt	11ec4b2896389484429edbabb5a717bd
VM34_20201002_235246.txt	99a4440ae9bab7f0de96d7656b4e739d
VM34_20201204_214820.txt	255f69007b253c7f2737b050c439f269
VM34_20210101_194641.txt	55e2e5308c1c818ab64e58b2952d63cc
VM34_20210205_184914.txt	3c1a1c1a8400464de6a4730d4e50f6c3
VM34_20210305_191848.txt	af6f78181173c9e7cad7e5f17029dd20
VM34_20210402_214448.txt	2fa8f197af888c6e0604ac9ca849aa1b
VM34_20210507_194658.txt	3a7e950b1d9e0d657a4a45e0b22506a5
VM34_20210604_190336.txt	30f1fe36c5ad4eac2a7ca5508663b9bf

5.6.11.3 RECOMMENDATION

Legislation should be considered that would require applications developed and utilized for voter rolls or voting to be developed to rigorous standards that ensure the confidentiality and integrity of the systems. Specifically, its recommended that the Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS) Level 3 be applied to all applications associated with voter rolls or voting and that it be required that this be fully validated no less than once every two years.

5.6.12 Double Scanned & Counted Ballots

Ballots Impacted 50

While examining batch discrepancies between the hand count and the Maricopa County Cast Vote Record (CVR) totals, we discovered that the county double counted ballots. We continue to review the Dominion images to identify the total number of double counted ballots. EVC4/10-26 thru 10-28/3385 which has a 50-ballot discrepancy is presented as an example below. The image shows one of 50 ballots that were tabulated twice giving each associated voter – two votes.

Tabulator 6004, BTC 288, Image 0154 (EV Batch 1377)

5.6.12.1 Data Files Utilized

File Name	MD5 Hash
Maricopa County Transfer Manifests	N/A
Maricopa County Daily Ballot Summary	N/A
Maricopa County 2020 General Election Cast Vote Record	c31a2f34714b7582cb17e907be3152e0

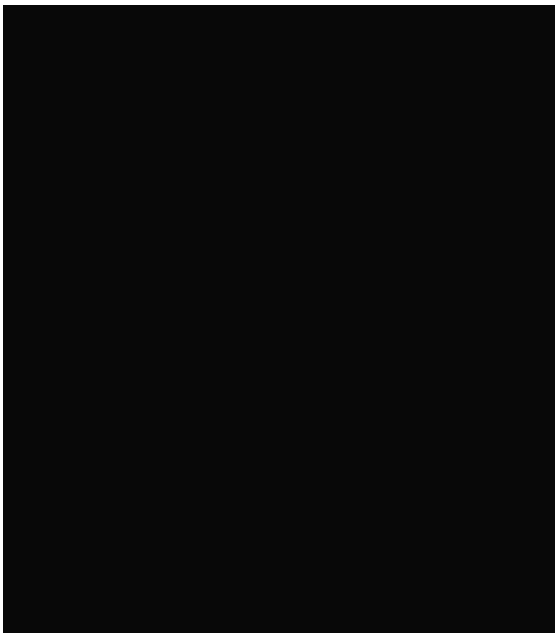
5.6.12.2 Recommendation

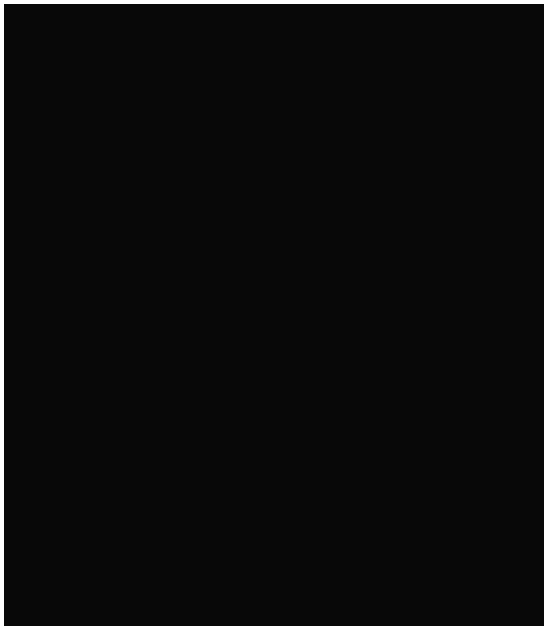
Maricopa County officials should audit the tabulation process daily to ensure no batches are scanned and tabulated multiple times.

5.6.13 UOCAVA Electronic Ballots Double Counted

Ballots Impacted 6

During our hand count, we identified multiple UOCAVA ballots that had been printed and duplicated more than once (e.g., Double Votes). Below is one example of one double printed UOCAVA ballot that was assigned two different serial numbers and submitted for duplication. This would result in two votes being counted for this one voter.





5.6.13.1 References

- EAC - 2018 UOCAVA Data Set [46]

5.6.13.2 Recommendation

Legislation should be considered which would require that systems utilized for UOCAVA would keep track of and help prevent the double-printing of ballots.

[46] https://www.eac.gov/research-and-data/datasets-codebooks-and-surveys

5.6.14 Duplicate Ballots Reuse Serial Numbers

Ballots Impacted 6

Duplicate Ballots were found reusing serial numbers. Without unique serial numbers its near impossible to match an original ballot (DSD) with its duplicated ballot (DUP).

Below is an example of a serial number used multiple times:

BOX ID	TYPE	SERIAL NO.
EVH1/11-11/DUP 175044	DUP	DUP294104
Original Damaged Ballots SD 8	DSD	DUP294104
Original Large Print Sent to Duplication 2	DSD	DUP294104
DSD RANDOM SAMPLE REVIEW 2	DSD	DUP171329
EVH1/11-07/DUP9582	DUP	DUP171329
Original Damaged Ballots SD 8	DSD	DUP171329

5.6.14.1 References

- State of Arizona – 2019 Elections Procedures Manual[47]
- A.R.S. § 16-621 – Proceedings at the counting center[48]

5.6.14.2 Recommendation

Legislation should be considered that would explicitly require each damaged ballot to have a unique serial number in order to match it up with its original.

[47] https://azsos.gov/sites/default/files/2019_ELECTIONS_PROCEDURES_MANUAL_APPROVED.pdf
[48] https://www.azleg.gov/ars/16/00621.htm

5.7 Informational Findings

5.7.1 Audit Interference

Ballots Impacted N/A

Runbeck Election Services is a privately owned company that provided election services including the printing of all mail ballots for Maricopa County in the 2020 General Election. Prior to the start of the audit, members of the audit team conducted research into the paper, ink, toner and format of the official ballots. As part of that research, the audit team contacted Runbeck CEO, to ask several general questions about the ballots used in the 2020 General Election. Initially, the CEO agreed to a call but then asked for the questions in writing. As requested, the audit team sent Mr. Ellington 5 general questions via email. Mr. Ellington responded to that email and said that Maricopa County instructed him that vendors, even private companies, should not speak with auditors. Maricopa County refused to provide the information about the ballot paper and ballot printing and then interfered with the auditor's communication with Runbeck, a private company that does business with hundreds of other jurisdictions and entities.

5.7.1.1 Recommendation

Legislators should consider legislation that would prohibit interference with legislative investigations under a criminal penalty.

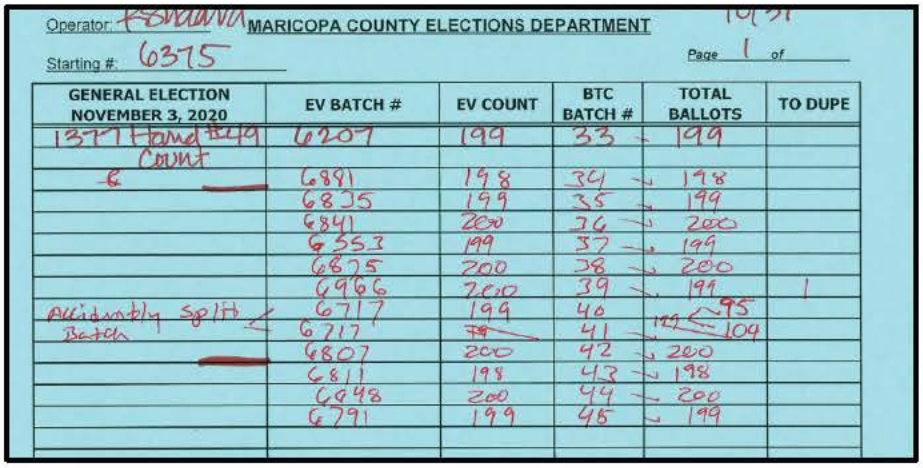
5.7.2 Batch Discrepancies

Ballots Impacted N/A

A comparison of our hand count totals to the CVR totals has revealed numerous discrepancies. We are in the process of comparing the Dominion images of ballots to determine the cause of the discrepancy. Below are two examples of discrepancies.

7	EVC1/10-31/6841 ✓		6841, 6835, 6553, 6875, 6966, 6717, 6807

Above: Maricopa County Ballot Transfer Manifest showing EV batches in the box.



Operator: [illegible] MARICOPA COUNTY ELECTIONS DEPARTMENT 10/31

Starting #: 6375 Page 1 of

GENERAL ELECTION NOVEMBER 3, 2020	EV BATCH #	EV COUNT	BTC BATCH #	TOTAL BALLOTS	TO DUPE
1377 Hand #49 Count	6207	199	33	199	
6	6881	198	34	198	
	6835	199	35	199	
	6841	200	36	200	
	6553	199	37	199	
	6875	200	38	200	
	6966	200	39	199	1
Accidentally split batch	6717	199	40	95	
	6717		41	104	
	6807	200	42	200	
	6811	198	43	198	
	6848	200	44	200	
	6791	199	45	199	

Above: Maricopa County Daily Ballot Summary for 10-31-2020 Tabulator C1. Note that BTC Batch 40 has 95 ballots and BTC Batch 41 has 104 ballots which combine to make up EV Batch 6717 which should have 199 total ballots.

tabu atorbatch d	tabu ator d	batch d	f e	ba ots
06001_00033	06001	00033	566	199
06001_00034	06001	00034	577	199
06001_00035	06001	00035	595	198
06001_00036	06001	00036	608	200
06001_00037	06001	00037	789	200
06001_00038	06001	00038	791	191
06001_00039	06001	00039	795	200
06001_00040	06001	00040	801	200
06001_00041	06001	00041	782	199
06001_00042	06001	00042	786	199
06001_00043	06001	00043	792	199
06001_00044	06001	00044	796	199

The CVR summary, pictured above, shows that BTC Batch 40 had 200 ballots tabulated and BTC Batch 41 had 199 ballots tabulated. These numbers do not match the Blue Sheet totals. Pallet 7 Box EVC1/10-31/6841 has only 1396 ballots but the CVR shows 1500 ballots. This results in a discrepancy of -104 ballots.

5.7.2.1 Data Files Utilized

File Name	MD5 Hash
Maricopa County Transfer Manifests	N/A
Maricopa County Daily Ballot Summary	N/A
Maricopa County 2020 General Election Cast Vote Record	c31a2f34714b7582cb17e907be3152e0

5.7.2.2 Recommendation

Maricopa County officials conduct daily audits and quality control measure to reduce errors.

5.7.3 Commingled Damaged and Original Ballots

Ballots Impacted N/A

The 2019 Election Procedure Manual requires that all original damaged ballots sent to duplication be placed in an envelope or container labeled "Ballots that have been duplicated." The County delivered boxes of ballots that were commingled and incorrectly identified. Batches identified on the manifest as original ballots were, in fact, machine duplicated ballots. The auditors could not rely on the County's description of ballot boxes or batches identified on the manifest. Hours of careful examination were required to unravel the inaccurate documents provided to ensure that votes were not counted twice.

As an example, in Box EVH1/11-07/MC17349, the manifest shows that there are 14 batches of original ballots. When the auditors opened the boxes to count the ballots, they observed 7 batches of original ballots, 8 batches of duplicate ballots and one batch missing from the manifest. Batches of duplicate ballots in boxes of original undamaged ballots is a difficult issue to unravel. During the hand count, we also identified several instances of damaged ballots in boxes with original ballots. We are unable to determine if the damaged ballots had been duplicated and tabulated as duplicates. The Election Procedures Manual makes it clear that damaged ballots sent to duplication must be separated and the County did not consistently adhere to this rule.

The Arizona Secretary of State claims that duplicate ballots and the original damaged ballots sent to duplication are to be segregated. In case No. CV2020-015285, Roopali Desai represented Arizona Secretary of State Katie Hobbs and said:

> *THE COURT: And those are segregated? I'm – those-- they don't get put in the pile where we're not going to be able to find them anymore, right? We know where those are?*
>
> *MS. DESAI: Duplicated ballots are -- those are --the original as well as the duplicated ballots are, by statute, segregated and preserved.*

5.7.3.1 References

- Arizona Supreme Court Case – CV2020-015285[49]
- State of Arizona – 2019 Elections Procedures Manual[50]

5.7.3.2 Recommendation

All duplicated ballots should be separated and properly identified as duplicates. All original damaged ballots sent to duplication should be separated and properly identified in compliance with the EPM.

[49] https://www.supremecourt.gov/DocketPDF/20/20-809/163521/20201211121632424_12-11-20%20Appendix%20Ward%20v%20Jackson.pdf
[50] https://azsos.gov/sites/default/files/2019_ELECTIONS_PROCEDURES_MANUAL_APPROVED.pdf

5.7.4 Early Votes Not Accounted for in EV33

Ballots Impacted N/A

The EV33 Early Voting Return Files do not contain entries for 255,326 Early Voters which are recorded in the VM55 Final Voted File. Individuals that vote as part of Early Voting, either by mail or in person, should have an EV33 entry related to their casting of a vote containing details as to when and how that vote was cast. Without an EV33 these details are unavailable, and it could make some types of audits impossible.

Ballot Type	Number of Voters
B – Early Vote - In-Person	38.817
R – Early Vote - Mail-In	187,823

NOTE: Please see Appendix S1 for a complete list of the entries from the VM55 file without EV33s.

5.7.4.1 References

- A.R.S. § 16-558.01 – Mailing of Ballots[51]
- A.R.S. § 16-246 – Early Balloting[52]
- A.R.S. § 16-542 – Request for ballot[53]

5.7.4.2 Data Files Utilized

File Name	MD5 Hash
EV33-1377-10-09-2020_101111.txt	f1daa7089f7300237f6b4ff779661cf9
EV33-1377-10-12-2020_113210.txt	72e4e6c102e3539b4dd15b4454357b69
EV33-1377-10-13-2020_111553.txt	9b14841281c031533322b50aabb86a24
EV33-1377-10-14-2020_112757.txt	1b7537d7d9b927dbf4e462ed5ee8f97c
EV33-1377-10-15-2020_121331.txt	dec7d08dde4970c26e32b8c844f4a9ab
EV33-1377-10-16-2020_113522.txt	f0a632c3fd9b5f177d48504dc119be31
EV33-1377-10-19-2020_111708.txt	db80b692a9188add0844a8974e227287
EV33-1377-10-20-2020_112351.txt	57d1795db8be71d516e29350e347fb3a
EV33-1377-10-21-2020_111843.txt	56c3b5a11651c68735164c578eade4e1
EV33-1377-10-22-2020_111714.txt	03551f170bf758efc90c013d0fe2e467
EV33-1377-10-23-2020_112614.txt	dbfdd369ac148723540c83f614cca454
EV33-1377-10-26-2020_111318.txt	0b68adff779f59c70a530000bf989aca
EV33-1377-10-27-2020_111413.txt	a6fc7377bf6c6fe6653f539c5970a6f7
EV33-1377-10-28-2020_111331.txt	43758b9290f90d0305d5ed84aa10becb
EV33-1377-10-29-2020_111300.txt	410b30b06f2ca73022f27173fe114038
EV33-1377-10-30-2020_111804.txt	5cb44e5ea214f40227e04345d4355ff7
EV33-1377-11-02-2020_111214.txt	5d15bb8686a022f53400550cfe010a07

[51] https://www.azleg.gov/ars/16/00558-01.htm
[52] https://www.azleg.gov/ars/16/00246.htm
[53] https://www.azleg.gov/ars/16/00542.htm

5.7.4.3 Recommendation

Legislation should be considered that requires that the various election related systems to properly integrate to give accurate and consistent counts between the mail-in ballots cast, mail-in ballots received, mail-in ballots accepted, mail-in ballots rejected, and be able to reconcile these details with who voted in the final voted file.

5.7.5 High Bleed-Through Rates on Ballots

Ballots Impacted N/A

A large number of the ballots from in-person voting, primarily on Election Day (ED), experienced bleed-through where the marks from one-side of the ballot were clearly visible on the other side of the ballot. This does not happen when the manufacturer recommended paper is utilized under normal circumstances.

The biggest concern with bleed through is if it occurs in a place that might somehow impact the reading of the ballot on the other side of the paper. Ballots are generally designed to minimize this potential by offsetting the races on each side of the paper so that if bleed-through does happen it is a safe distance away from the ballot ovals on the other side of the paper. Maricopa County Ballots were designed in this manner.

The effect of this offsetting can be hampered, however, if the ballot printer is not in calibration (Please see Section 5.7.10, “Out of Calibration Ballot Printers”). When this occurs the miscalibration causes the front of the ballot to not align where it was intended to on the back of the ballot. If this miscalibration is off enough it could allow the bleed-through to fill out a ballot oval on the other side of the paper and cast a vote, cause an overvote, or simply confuse the tabulator enough to send the ballot to adjudication. Out of the several thousand ballot images that were manually reviewed we could not find any images where bleed-through was close enough to a ballot oval to cause mistabulation, nor did we see any immediate correlation with adjudication. The Dominion tabulators appeared to focus on the actual oval and no bleed-through example was found where a ballot printer was so miscalibrated it actually filled a portion of the oval.

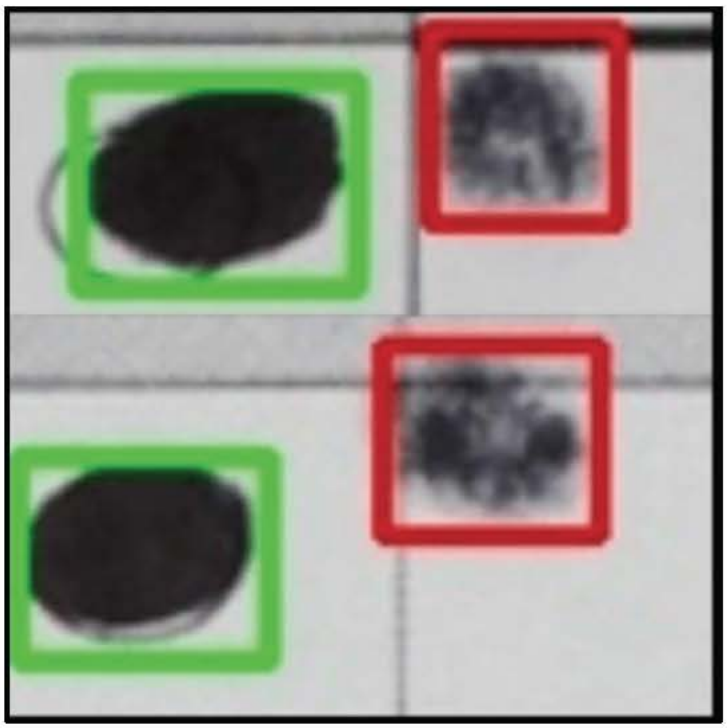


Figure 1 - Green is around the actual vote. The red boxes show the bleed through from the other side.

5.7.5.1 References

- Dominion Printing & Finishing Specifications[54]

5.7.5.2 Recommendation

Legislation should be considered that would require that the election equipment be properly maintained, including, but not limited to ensuring that ballot printers are in the proper calibration.

6.7.5.3Instances

Kinematic Artifact processing is currently evaluating the ballot images to do a full analysis of bleed-through. A full report documenting all of the bleed-through is expected in the coming weeks. At this time, this particular issue appears to be systemic to any non-Runbeck printed ballots.

[54] https://www.sos.state.co.us/pubs/elections/VotingSystems/DVS-DemocracySuite511/documentation/SD-IC-PrintingSpecification-5-11-CO.pdf

5.7.6 Improper Paper Utilized

Ballots Impacted N/A

A large number of the ballots from in-person voting, utilized paper that is not recommended by the manufacturer of the tabulators for use in the systems. This can result in higher jam rates, more bleed through, and could theoretically impact the readability of the ballots by the scanners, but this last case is extremely unlikely. At this time 10 different papers have been found. Several of these paper stocks include paper with the weight from 20lb to 30lbs; when the generally accepted best practice for voting is to utilize ballot stock of 80lbs or higher. Since this type of paper is generally not tested within the equipment, nor part of the Logic and Accuracy testing, the effects of utilizing it is unclear.

The large number of papers utilized during this election and the lack of official reporting about what paper stocks were utilized made it difficult to identify any potential counterfeit ballots. Standardization on these details would more greatly facilitate future audits.

5.7.6.1 References

- Dominion Printing & Finishing Specifications[55]

5.7.6.2 Recommendation

Legislation should be considered that would require that paper stocks utilized on election day should conform to manufacturer recommendations to ensure that the paper that has been tested in the device is what is actually utilized to cast votes. Legislation should also be considered that mandates the standardization of paper utilized for the election including requiring that the ballot stock amounts utilized be fully accounted for and tracked.

5.7.6.3 Instances

Kinematic Artifact processing is currently evaluating the ballot images to do a full analysis of types of paper utilized. A full report documenting all of the papers utilized is expected in the coming weeks.

[55] https://www.sos.state.co.us/pubs/elections/VotingSystems/DVS-DemocracySuite511/documentation/SD-IC-PrintingSpecification-5-11-CO.pdf

5.7.7 Inaccurate Identification of UOCAVA Ballots

Ballots Impacted N/A

Maricopa County identified only one box on the manifest as having UOCAVA Original Ballots sent to duplication. The audit team examined all other boxes of ballots and identified 6 other boxes that were inaccurately labeled. All UOCAVA ballots identified by the County were 8 ½" X 11" copies of electronically submitted voted ballots. UOCAVA ballots were found in boxed labeled Braille Ballots and boxes labeled the generic Original Ballots/Damaged/Sent to Duplication. This inaccurate labeling of UOCAVA boxes gave the impression that there were far fewer UOCAVA ballots than were actually counted.

Ballot Custody Transfer Manifest
Arizona Senate Fifty-Fifth Arizona Legislature / First Regular Session Subpoena Duces Tecum
Karen Fann, President of the Arizona Senate / Warren Petersen, Chairman of Senate Judiciary Committee

Transfer Date: 3/3/2021
Total Boxes [redacted]
Observed by:

Pallet #	Box # (Ballot Type, Machine, Date, First Batch)		Batches
41	[redacted]	✓ 1	Original Ballots/Damaged/Sent to Duplication
41		✓ 2	Original Ballots/Damaged/Sent to Duplication
41		✓ 3	Original Ballots/Damaged/Sent to Duplication
41		✓ 4	Original Ballots/Damaged/Sent to Duplication
41		✓ 5	Original Ballots/Damaged/Sent to Duplication
41		✓ 6	Original Ballots/Damaged/Sent to Duplication
41		✓ 7	Original Ballots/Damaged/Sent to Duplication
41		✓ 8	Original Ballots/Damaged/Sent to Duplication
41		✓ 9	Original Ballots/Damaged/Sent to Duplication
41		✓ 10	Original Ballots/Damaged/Sent to Duplication
41		✓ 11	Original Ballots/Damaged/Sent to Duplication
41		✓ 12	Original Ballots/Damaged/Sent to Duplication
41		✓ 13	Original Ballots/Damaged/Sent to Duplication
41		✓ 14	Original Ballots/Damaged/Sent to Duplication
41		✓ 15	Original Ballots/Damaged/Sent to Duplication
41		✓ 16	Original Ballots/Damaged/Sent to Duplication
41		✓ 1	Braille Original to Duplication
41		✓ 2	Braille Original to Duplication
41		✓ 3	Braille Original to Duplication
41		✓ 1	Large Print Original to Duplication
41		✓ 2	Large Print Original to Duplication
41		✓ 3	Large Print Original to Duplication
41		✓ 1	Election Day Damaged Original to Duplication
41		✓ 1	Provisional Damaged Original to Duplication
41		✓ 1	UOCAVA Original to Duplication
41		✓ 1	Data Cards - ICP2s - Election Day/USB Drives for Results Upload
41		✓ 2	Totals Tapes - ICP2s - Election Day
41		✓ 3	Totals Tapes - ICP2s - Election Day
41		✓ 4	Original Damaged Ballots for Duplication - Random Sample Review #1 (Box 1 of 2)
41		✓ 5	Original Damaged Ballots for Duplication - Random Sample Review #1 (Box 2 of 2)
41		✓ 6	Original Damaged Ballots for Duplication - Random Sample Review #2 (Box 1 of 2)

[redacted] ✓ Orig Dam Ballots for Dupl - Rand Samp Rev #2 Box 2 of 2 CN

[redacted] 4/22/2021 [redacted]

5.7.7.1 Recommendation

Legislation should be considered that requires UOCAVA systems to be designed in a manner to prevent potential multiple copies of UOCAVA ballots from being printed.

5.7.8 Missing Subpoena Items

Ballots Impacted N/A

The original subpoena dated January 13, 2021, required Maricopa County to provide "Access to all original, paper ballots (including but not limited to early ballots, Election Day Ballots and Provisional Ballots)." The auditors did not receive the following original ballots:

- Rejected Provisional Ballots
- Uncured Mail Ballots
- Ballots returned to the County as undeliverable

Failing to receive these components prevented portions of the audit from being completed, such as validating that the right number of provisional ballots existed, and that ballots returned to the County as undeliverable were properly accounted for and were not reused in some other context. Since these items were not provided, this work was not able to be completed.

5.7.9 No Record of Voters in Commercial Database

Ballots Impacted N/A

All voters within the Final Voted File, or VM55, was cross-checked against a commercially available data source provided by Melissa[56] called Personator and 86,391 individuals were found with no record in the database for either their name, or anyone with the same last name at the address in the VM55 file. It is expected that most if not all of these individuals are in fact real people with a limited public record and commercial presence. It is highly recommended that this list be further validated with canvassing to determine what percentage of these voters represent current and valid voters.

Personator is a best-in-class identity and address validation tool. It confirms that an individual is associated with an address, indicates prior and current addresses, tracks when and where the individual moves, tracks date-of-birth and date-of-death. To accomplish this, it utilized both private and government data sources such as the US Postal Service's National Change of Address (NCOA) service, and the Social Security Administration's Master Death List.

NOTE: The following chart illustrates the percentage of voters by registered party that the Ballot Impacted number represents. This should give a rough idea on the impact to the electorate if the votes were cast by the voters and not another individual that was somehow able to cast a vote.

Party	%
Democrat Party	43.97%
Prefer Not to Declare	29.83%
Republican Party	22.21%
Independent	2.55%
Libertarian Party	1.3%
Green Party	0.12%

5.7.9.1 Data Files Utilized

File Name	MD5 Hash
Maricopa County-VM55 Final Voted Nov2020 PBRQ	43070bc7afdf40a37cd45092e9733654

[56] https://www.melissa.com

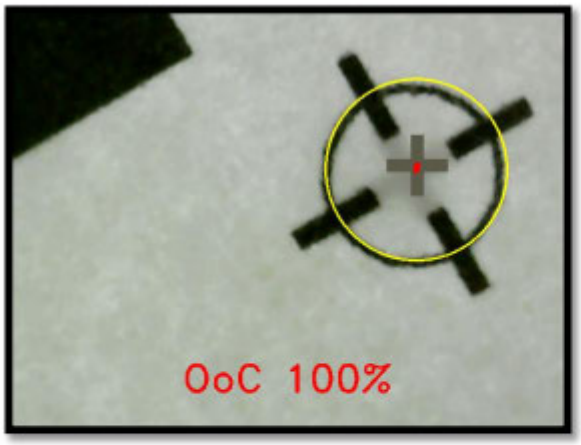
5.7.9.2 RECOMMENDATION

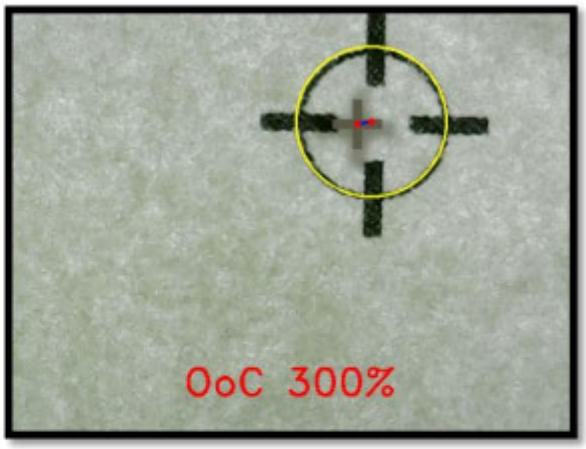
Legislation should be considered that requires a periodic review and maintaining of the voter rolls to be sure it represents current Arizona residents.

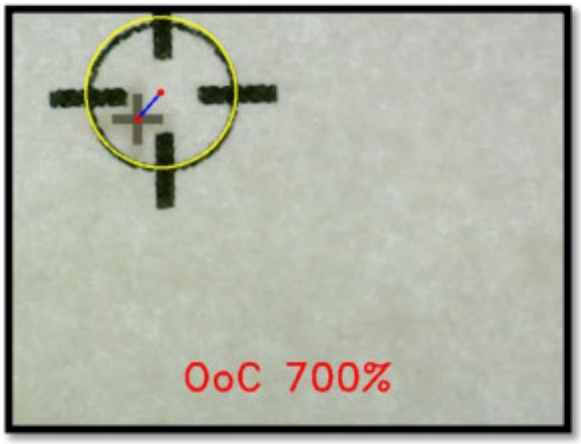
5.7.10 OUT OF CALIBRATION BALLOT PRINTERS

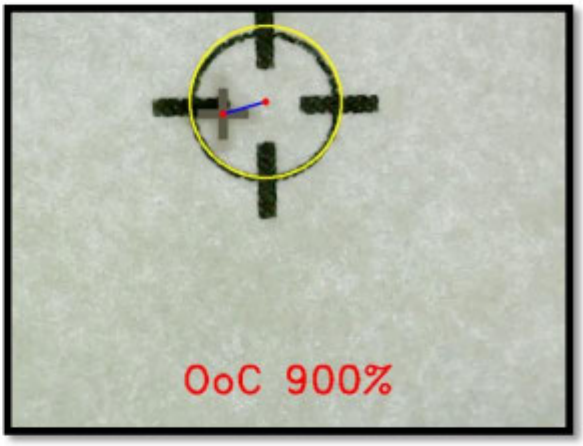
Ballots Impacted N/A

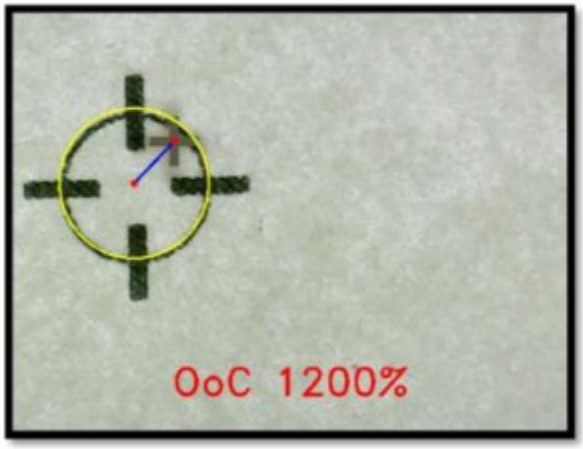
A large number of ballots appear to have been printed on printers not properly calibrated. This means that the front-page of the ballot is not consistently aligned with the back page of the ballot. The way this alignment presented appeared to be unique for each vote center printer. This is contrary to manufacturer guidelines and recommendations and could theoretically result in inconstant reading of votes across all the different tabulators, although we identified no instances of this issue causing a ballot to be tabulated incorrectly in the several thousand images reviewed.

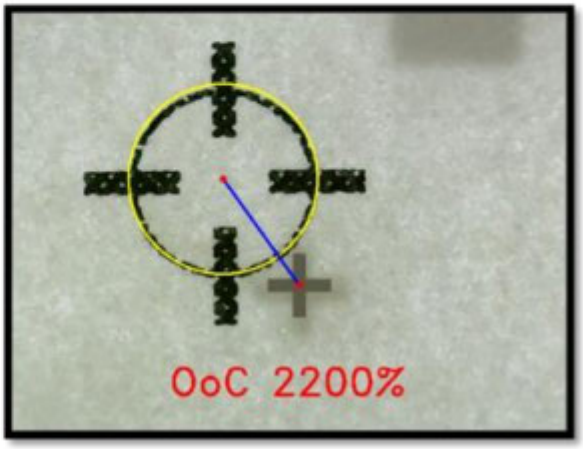

OoC 100%


OoC 300%


OoC 700%


OoC 900%


OoC 1200%


OoC 2200%

5.7.10.1 References

- Dominion Printing & Finishing Specifications[57]

5.7.10.2 Recommendation

Legislation should be considered that would require that the election equipment be properly maintained, including, but not limited to ensuring that ballot printers are properly calibrated.

5.7.10.3 Instances

The Kinematic Artifact processing is currently processing ballot images to fully map all printer miscalibrations. A full report is expected in the coming weeks.

5.7.11 Real-Time Provisional Ballots

Ballots Impacted N/A

The Arizona Secretary of State Elections Procedures Manual identifies circumstances that require the issuance of a Provisional Ballot. If a voter appears in the e-pollbook or signature roster as having received an early ballot by mail, but the voter wants to vote in person on Election Day, that voter must be issued a Provisional Ballot. However, Maricopa County reported 58,550 voters who had received mail ballots but were issued standard ballots on Election Day. The County identifies these as "real-time Provisional Ballots." There is no mention of real-time provisional in the AZ Elections Procedures Manual. In fact, the EPM specifically addresses this circumstance and is clear that such voters must be issued a Provisional ballot.

There appears to be no statutory authority for Maricopa County to deviate from the EPM and issue standard ballots to voters who had already received a mail ballot. We identified no instances of these voters casting more than one ballot, however.

This was reported as a note at the bottom of page 12,329 of the November General Election Canvass Final -below:

> **Note:** There were 58550 Early Ballot recepients that had not RETURNED their Early Ballot and consequently were issued a standard ballot on Election Day. These were processed as real-time Provisional Ballots.

A.R.S. § 16-579(F). Issuing a Provisional Ballot

1. *Circumstances Requiring Issuance of a Provisional Ballot:*
   Voter Received an Early Ballot
   A voter must be allowed to vote a provisional ballot if the voter appears on the signature roster or e-pollbook as having received an early ballot-by-mail, but either:
   (1) affirms that they have not voted and will not vote the ballot-by-mail; or
   (2) surrenders the ballot-by-mail to the inspector on Election Day. A.R.S. § 16-579(B)
   Voters who appear at a voting location with a ballot-by-mail that has not been voted, along with the affidavit envelope, may use a privacy booth at the voting location to mark the ballot-by-mail. In this circumstance, the voter

[57] https://www.sos.state.co.us/pubs/elections/VotingSystems/DVS-DemocracySuite511/documentation/SD-IC-PrintingSpecification-5-11-CO.pdf

does not sign in and the voter must place the voted ballot-by-mail in its affidavit envelope, sign the affidavit envelope, and place the envelope in the early ballot drop-off container at the voting location.

5.7.11.1 References

- State of Arizona – 2019 Elections Procedures Manual[58]
- A.R.S § 16-579 – Procedure for obtaining ballot by elector[59]

5.7.11.2 Data Files Utilized

File Name	MD5 Hash
11-03-2020-0 Canvass COMPLETE NOV2020	ce62cc061b6bb56b4fd40aa4866adb16

5.7.11.3 Recommendation

Maricopa County should explain this deviation from the Elections Procedures Manual.

5.7.12 Voter Registration System Audit Access

Ballots Impacted N/A

One of the most important components of the audit was the analysis of the voter registration system and records of authorized or unauthorized access to that system. Our audit team has been denied the access required to complete this portion of the audit. In the Senate's subpoena dated January 12, 2021, Maricopa County was ordered to provide the auditors access to, or control of all equipment used in connection with the administration of the 2020 election. In a second subpoena, dated July 26, 2021, the County was ordered to provide all reports, finding and other documents concerning the voter registration breach. The response from the County claims that they are not aware of a breach.

> **1. "All reports, findings and other documents concerning any breach of the voter registration server, the Maricopa County Recorder's Office systems, or any other aspect of the Maricopa County elections systems at any time within six months of the November 3, 2020 general election"**
>
> The Board of Supervisors is not aware of any "breach", as stated above, occurring during this time period, or any other time period relevant to the November 3, 2020 election. The Board of Supervisors is aware of an incident in November 2020 wherein an individual programmatically accessed the County Recorder's website and gathered publicly available information for a short period of time. The Recorder's website is in no way connected to the air-gapped tabulation system in the secure room where ballots are counted. To the extent you are requesting records related to this incident, you recently made a public records request to both the Maricopa County Recorder and the Board of Supervisors requesting similar information. As always, the Board of Supervisors will comply with your public records request promptly consistent with Arizona law. We hereby request that you accept our response to your public records request in lieu of production pursuant to this subpoena.

Claiming that this breach was nothing more than unauthorized access to public data has not been supported with evidence. According to a news article published December 4th, 2020, Maricopa County confirmed voter data had been stolen and that a federal investigation was under way. CISA considers voter registration systems to be critical infrastructure and thus requires states and counties to implement the highest levels of security. The only way to ensure that there is one vote for every legally registered voter is careful control of the voter registration database.

[58] https://azsos.gov/sites/default/files/2019_ELECTIONS_PROCEDURES_MANUAL_APPROVED.pdf
[59] https://www.azleg.gov/ars/16/00579.htm

5.7.12.1 References

- Maricopa County Letter to Arizona Senate[60]
- Cybersecurity and Infrastructure Agency (CISA)[61]

5.7.12.2 Recommendation

Legislation should be considered that would require applications developed and utilized for voter rolls or voting to be developed to rigorous standards that ensure the confidentiality and integrity of the systems. Specifically, its recommended that the Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS) Level 3 be applied to all applications associated with voter rolls or voting and that it be required that this be fully validated no less than once every two years.

5.7.13 Questionable Ballots

Ballots Impacted	N/A

Analysis of the paper ballots has discovered ballots which exhibit characteristics that are anomalous and do not match known legitimate ballots. This includes color ballots that are missing Machine Identification Codes (MIC), as well as ballots that are demonstrating consistent printing irregularities that suggest they were not printed with the standard ballot PDF generated from the Dominion Election Management System (EMS). These irregularities may have logical explanations, but these explanations are not immediately evident.

NOTE: The questionable ballots have been reviewed to determine if they favor one presidential candidate over another presidential candidate. No discernable pattern could be determined. This highly suggests that these are not counterfeit but do require some sort of explanation.

5.7.13.1 References

- Maricopa County Election Facts and Myths[62]
- Runbeck Printing Website[63]
- HP PageWide WebPress T HD Specification[64]

5.7.13.2 Recommendation

Legislators should consider passing laws standardizing the papers and printing process utilized for printing ballots and requiring documentation to be kept of all papers utilized. This will facilitate determining if a ballot is in fact genuine and remove any areas for confusion.

[60] https://www.maricopa.gov/DocumentCenter/View/70435/Final-Signed-Letter-to-Senators
[61] https://www.cisa.gov/election-security
[62] https://recorder.maricopa.gov/justthefacts/
[63] https://runbeck.net/election-solutions/election-printing-mailing/
[64] https://www.hp.com/us-en/commercial-industrial-printing/pagewide/t250-hd-web-presses.html

6 Voting Machine Findings

The following section outlines all findings related to the voting machines including the analysis and discoveries during the Voting Machine phases of the work.

6.1 Voting Machine Scoring

Cyber Ninjas utilizes a risk ranking system based on the guidelines outlined by NIST publication 800-30, "Guide for Conducting Risk Assessments – Information Security." A severity is assigned to a finding based on a combination of the likelihood the finding could impact the election, or the ability to audit the election and the impact it could have on the election results.

	Impact			
Likelihood	**Low**	**Medium**	**High**	**Critical**
Critical	Medium	High	High	Critical
High	Medium	Medium	High	High
Medium	Low	Medium	Medium	High
Low	Low	Low	Medium	Medium

Table 1: Election Risk Matrix.

Both the likelihood and the impact of the finding are rated independently on a scale from "Low" to "Critical." These ratings are then combined utilizing the risk matrix represented in Table 1 to determine the associated severity for the issue.

6.2 Digital Analysis Summary

Because the Maricopa County Board of Supervisors and the Arizona State Senate have recently settled their dispute concerning outstanding subpoena items, this portion of the audit is not yet complete. Analysis of those items that were produced, however, clearly demonstrated that the Maricopa County voting systems did not follow CISA or industry standard cyber security best practices.

First Maricopa County personnel did not control the administrative iButton credentials necessary to configure, validate and certify the ICP2 tabulators. Second, Maricopa County did not properly assign and manage the user names and passwords necessary to restrict access the voting systems. The user accounts were not attributable to an individual, rather they were shared throughout the staff. Furthermore, the same password was utilized by multiple accounts and was never changed since the installation of the Dominion software. That same password was used by both administrative and user accounts. If a user had access to user level account, that user had all the knowledge necessary to perform administrative functions with elevated access. Third, the windows security and activity logs were not preserved for the required 22 months following the election, thus significantly hampering the analysis of authorized activity. It did appear that the Dominion software specific logs were preserved, but those logs do did not provide the same level of detail or data that the Windows operating system logs did for security events, remote login events or other user activity. Fourth, there was a clear lapse in the hardware configuration monitoring and baseline in the Maricopa County voting systems as evidenced by the presence of an unauthorized second bootable hard drive in the Adjudication 2 workstation.

6.3 Summary Table

#	Finding Name	Likelihood	Impact	Severity
6.4.1	Election Management System Database Purged	High	High	High
6.4.2	Election Files Deleted	High	High	High
6.4.3	Corrupt Ballot Images	High	High	High

6.5.1	Missing Ballot Images	Medium	High	Medium
6.5.2	Failure to Follow Basic Cyber Security Practices	Medium	High	Medium
6.5.3	Subpoenaed Equipment Not Provided	Medium	High	Medium
6.5.4	Anonymous Logins	Medium	Medium	Medium
6.5.5	Dual Boot System Discovered	Medium	Medium	Medium
6.5.6	EMS Operating System Logs Not Preserved	Low	High	Medium
0	Election Data Found from Other States	Low	Medium	Low

6.4 High Findings

6.4.1 Election Management System Database Purged

Likelihood: High **Impact:** High

The Election Management System (EMS) database which holds all details associated with the 2020 General Election was purged and all the election results were cleared by a Results Tally and Reporting Admin on February 2 at 5:14 pm; the evening before the Pro V & V audit was scheduled to officially start. This means that these results were not available for Pro V & V or SLI to perform any type of audit, nor were they available for Cyber Ninjas to review. The next day Pro V & V then proceeded to add new tabulators for their audit, and they imported results into these tabulators further clearing remnants of the database. It is worth noting that the Dominion software fully supports creating a full copy of an existing election project; and if a cleared database was required for Pro V & V to perform their audit, they could have first duplicated the existing Election Project. Neither of the "auditors" retained by Maricopa County identified this finding in their reports.

NOTE: While the log file clearly indicates that the results and images were also purged as part of the process, the majority of the images did appear to be reloaded back to the system at some point. There were images missing and a number of corrupt images as can be seen in the other findings.

NOTE: On August 26th the Maricopa County Board of Supervisors was requested to explain the reasoning for this activity but has chosen not to respond.

[redacted]

Figure 2 - UserLog shows that RTRAdmin Successfully Purged the 20201103 Election Database and Files.

Tabulator Nu...	Name	Location	Type	Counting Group	Log File	Closed	Images Loaded	Load
157189	Audit 7	Maricopa	ICE/ICP 2	EARLY VOTE	☐	☑	☑	1
3002	HiPro 2 Early ...	MCTEC	Imagecast Ce...	EARLY VOTE	☐	☐	☐	1
157192	Audit 10	Maricopa	ICE/ICP 2	EARLY VOTE	☐	☑	☑	1
157191	Audit 9	Maricopa	ICE/ICP 2	EARLY VOTE	☐	☑	☑	1
157193	Audit 11	Maricopa	ICE/ICP 2	EARLY VOTE	☑	☑	☑	1
157185	Audit 3	Maricopa	ICE/ICP 2	EARLY VOTE	☐	☑	☑	1
157186	Audit 4	Maricopa	ICE/ICP 2	EARLY VOTE	☐	☑	☑	1
157195	Audit 13	Maricopa	ICE/ICP 2	EARLY VOTE	☐	☑	☑	1
6004	Canon 4 Early...	MCTEC	Imagecast Ce...	EARLY VOTE	☐	☐	☐	1
157190	Audit 8	Maricopa	ICE/ICP 2	EARLY VOTE	☐	☑	☑	1
157184	Audit 2	Maricopa	ICE/ICP 2	EARLY VOTE	☐	☑	☑	1
157187	Audit 5	Maricopa	ICE/ICP 2	EARLY VOTE	☐	☑	☑	1
157188	Audit 6	Maricopa	ICE/ICP 2	EARLY VOTE	☐	☑	☑	1
157194	Audit 12	Maricopa	ICE/ICP 2	EARLY VOTE	☐	☑	☑	1
157183	Audit 1	Maricopa	ICE/ICP 2	EARLY VOTE	☐	☑	☑	1
3001	HiPro 1 Early ...	MCTEC	Imagecast Ce...	EARLY VOTE	☐	☐	☐	3

Figure 3 - Tabulator List is full of "audit" tabulators which are the only ones with results.

Page: 1 of 62

Election Summary Report
General Election
Maricopa County
November 3, 2020

Elector Group	Counting Group	Ballots	Voters	Registered Voters	Turnout
Total	EARLY VOTE	8,164	8,164		0.31%
	ELECTION DAY	0	0		0.00%
	PROVISIONAL	0	0		0.00%
	Total	8,164	8,164	2,595,272	0.31%

Registered Voters: 8,164 of 2,595,272 (0.31%)
Ballots Cast: 8,164

Figure 4 - Results for the 2020 General Election only show 8,164 votes from the Pro V & V audit.

6.4.1.1 Data Files Utilized

File Name	MD5 Hash
AZAud-E-089-1 _EMS PRIMARY\AZAud-E-089-1 _EMS PRIMARY	95a6f531c4969dda8f5703858e33d414

6.4.1.2 Recommendation

Legislation should be considered that could more greatly facilitate audits to be performed and require the counties to cooperate with the audits when they occur. Specifically, the county should be required to provide all the details needed to have a fully functional Election Management System where results can be reviewed.

6.4.2 Election Files Deleted

Likelihood: High **Impact:** High

According to the Master File Table (MFT) of the drives, a large number of files on the Election Management System (EMS) Server and HiPro Scanner machines were deleted including ballot images, election related databases, result files, and log files. These files would have aided in our review and analysis of the election systems as part of the audit. The deletion of these files significantly slowed down much of the analysis of these machines. Neither of the "auditors" retained by Maricopa County identified this finding in their reports.

6.4.2.1.1 Deletion Activity on the EMS C:\ Drive

The EMS server that was produced contained six hard drives. Two of those hard drives were configured in a mirrored configuration and contained the operating system and install programs. This mirrored drive was assigned the drive letter "C" and was the boot drive for the EMS. Between 10/28/20 08:52:36AM and 11/05/20 05:58:58PM 865 directories and 85,673 election related files (scanned ballots, .dvd files, slog.txt files, etc.) were deleted from the EMS C:\ drive. A full listing is provided in the file named Files and Directories Deleted from the EMS C Drive.txt.

Figure 5-Example of Election Related File Deletion from EMS C:\ Drive

6.4.2.1.2 Deletion Activity on the EMS D:\ Drive

The other four (4) hard drives were configured in a 0+1 hardware raid configuration that contained a single 2.1 Terabyte partition. For the purposes of this examination this raid was manually reconstructed and mounted as a single 2.1 TB drive. This mounted image was then imaged using the FTK Imager software package. The resulting forensic image was then utilized for analysis. This drive contained the dominion election data, election definitions, the election databases, the NAS directory and the scanned ballot images. Between 11/01/20 10:37:41AM and 03/16/21 10:17:06AM 9,571 directories and 1,064,746 election related files were deleted from the D drive. These deleted files include scanned ballot images, ICX results, context.spx files, choice.spx files, .dvd files from the tabulators, and other election related files. A full listing of the deletions is provided in the file Files and Directories Deleted from the EMS D Drive.txt.

Figure 6-Trump Ballot Image Created and Deleted on 1 Nov 2020 from D:\ Drive

Figure 7-Deleted Election Results Files on 5 November 2020 from D:\ Drive

6.4.2.1.3 Deleted Directories and Files from HiPro 1

HiPro 1 Deleted Files and Folders – 304 Directories and 59,387 files containing election data were deleted from the HiPro scanner number 3 (CyFIR evidence number AZAUD-C-096) by an individual using the account hipradmin01. These files were deleted on 3 March 2021 between 03/03/21 12:53:34PM and 03/03/21 01:37:49PM.

Figure 8-Deleted Election Related Files from HiPro 1

6.4.2.1.4 Deleted Directories and Files from HiPro 3

HiPro 3 Deleted Files and Folders – 1,016 Directories and 196,463 files containing election data were deleted from the HiPro scanner number 3 (CyFIR evidence number AZAUD-C-099) by an individual using the account hipradmin03. These files were deleted on 3 March 2021 between 03/03/21 01:26:32PM and 03/03/21 01:37:49PM.

[redacted]

Figure 9-Deleted Election Related Files from HiPro3

6.4.2.1.5 Deleted Directories and Files from HiPro 4

HiPro 4 Deleted Files and Folders – 981 Directories and 191,295 files containing election data were deleted from the HiPro scanner number 4 (CyFIR evidence number AZAUD-C-098) by and individual using the hiproadmin04 account. These files were deleted on 3 March 2021 between 03/03/21 02:32:47PM and 03/03/21 02:44:32PM.

[redacted]

Figure 10-Deleted Election Related Files on HiPro4

6.4.3 Corrupt Ballot Images

Likelihood: High **Impact:** High

The audit has discovered 263,139 ballot images on the election system that are corrupt and unreadable TIFF format images. It is unclear what events could have resulted in this number of images being corrupted. The corruption of the ballot images in the election system only occurs for ballots that were scanned on or after November 1, 2020. No corruption of ballot images occurred in the 1,347,240 ballots processed on the same nine high-speed scanners prior to November 1, 2020. The image corruption is incongruous with the performance of those same nine high-speed scanner systems during the entire election prior to November 1, 2020. For each of the eight high-speed scanners used for ballots scanned starting on November 1, approximately half of the TIFF images are corrupted. The corruption prevents the audit team from confirming the efficacy of the vote totals and the correlation to the paper ballots stored in the various batches.

TIFF image batches were corrupted in some way and not entirely readable for the purposes of the audit. This means that it was impossible to confirm that the electronically recorded votes corresponded to the corrupted TIFF ballot images. In this scenario it is possible that manipulation of the electronic vote totals occurred in the instances where the TIFF images are corrupted. These corrupt TIFF images are not in the folder structure where finally adjudicated ballots are held. Instead, the corrupted adjudicated ballots for “Early Vote Spare 2” are located amongst what appear to be test batch ballot images.

NOTE: Because these images are critical, a new copy of these images was requested from Maricopa County, but a response was not given.

Figure 11 - Early Vote Spare 2 Misallocated and Corrupted Ballots.

Figure 12 - HiPro 1 Early Vote Spare 2 Showing 97,098 Ballot Tiff Images, Showing the High Volume on these Devices.

[redacted]

Figure 13 - Example folder showing corrupt TIFF images. The corrupt images either will not display a pre-view at all, or the ballot will be partially blacked out.

In addition, the very same nine (9) high speed tabulators processed more than 1.3 million votes from October 20, 2020, to October 31, 2020 without corrupting any TIFF ballot images. It is anomalous that these high-speed scanners had no errors for the eleven-day period prior to November 1, 2020, but had issues starting on November 1.

NOTE: The top level of the EMS folder structure containing all of the scanner's zip files with the unadjudicated ballots (except the aforementioned missing ballots) are present. The corrupted ballots by file name do appear in these zip files, but none of the ballots in this folder structure are adjudicated.

6.4.3.1 Data Files Utilized

File Name	MD5 Hash
AZAud-E-089-1 _EMS PRIMARY\AZAud-E-089-1 _EMS PRIMARY	95a6f531c4969dda8f5703858e33d414

6.4.3.2 Reproduction Steps

In order to locate and find the corrupt ballots, the Unix "find" command can be employed in conjunction with the "file," "grep," and "wc" (word count) command to determine if the ballot image is indeed a valid TIFF image format file.

For example, here is the command line:

[redacted]

6.4.3.3 Recommendation

Legislation should be considered that will make ballot images an artifact from an election that is publicly published for increased transparency and accountability in the election process.

6.5 Medium Finding

6.5.1 Missing Ballot Images

Likelihood: Medium **Impact:** High

The total number of ballot images that exist within the body of computer forensics material provided for the audit is substantially less than the official vote totals and the total number of paper ballots audited. 21,273 ballot images are entirely missing from the forensics images of the election equipment. This means that there are electronic votes recorded, but no actual ballot images that correspond to the votes. This makes it impossible to fully validate the results or confirm that the Election Management System (EMS) was not tampered with.

The results from the high-speed scanners from 11/1 to 11/13 are not found in the folder named, “20201103 General ballots and election files and adjudicated tabulators.” We find the bulk of them in “20201103 General\Results” folder. The first 15-20 (depending on the specific high-speed scanner) of these batches do not have ballot images. The total number of missing ballot images is 21,273.

Figure 14 - The tabulator results are found in two different folders, "20201103 General Ballots and election files and adjudicated tabulators" and "20201103 General.”

[redacted]

Figure 15 - The tabulator folder that should have images within it does not have any images. In total 21,273 images were missing.

6.5.1.1 Data Files Utilized

File Name	MD5 Hash
AZAud-E-089-1 _EMS PRIMARY\AZAud-E-089-1 _EMS PRIMARY	95a6f531c4969dda8f5703858e33d414

6.5.1.2 Reproduction Steps

In order to find the number of ballot images, first it is necessary to query the EMS database for the election project name Project 20201103 General and select the vote total for the entire election using the following MS SQL command. This query is executed using the Microsoft SQL Server Management Studio v17.1 that was found to be installed on the EMS.

Windows Domain and Logon: [redacted]

Database Name: [redacted]

[redacted]

In order to count the total number of ballot images, the Unix "find" command can be employed in conjunction with the "grep" and the "wc" (word count) command to determine if the ballot image is indeed a valid TIFF image format file.

For example, here is the command line:

[redacted]

Add these totals together and this is the total number of TIFF images on the EMS for the election.

Then take the total number of ballots from the EMS from and subtract the total from the above commands.

6.5.1.3 RECOMMENDATION

Legislation should be considered that will make ballot images an artifact from an election that is publicly published for increased transparency and accountability in the election process.

6.5.2 FAILURE TO FOLLOW BASIC CYBER SECURITY PRACTICES

Likelihood: Medium **Impact:** High

The Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) has published a series of cybersecurity best practices and guidelines. In addition to general guidelines, CISA has also published specific best practices for securing election systems that is available for all counties to access at no cost. In the most recent version of the document CISA broke this guidance into specific categories for ease of utilization. As part of these findings, this report will address the following CISA recommendations and address the lack of Maricopa County compliance with the recommendations; Software and Patch Management, Log Management, Credential Management, and Establish a Baseline for Host and Network Activity.

6.5.2.1 INSTANCES

6.5.2.1.1 Software and Patch Management

CISA outlines the necessity for software and patch management within election systems. Specifically, CISA states "Failure to deploy patches in a timely manner can make an organization a target of opportunity, even for less sophisticated actors, increasing the risk of compromise." It is clear that there was no established program to patch the operating system or even update the antivirus definitions. Neither the operating system nor the antivirus had been patched or updated since August 2019 (the date of the installation of the Democracy Suite). The county released a statement that they were prohibited from updating the operating system, that had they done so it would have invalidated the certification issued by the Voter Assistance Commission (VAC) for the Dominion software. This statement is contradicted by the County's own actions following the installation of the Dominion software. Contrary to the claims that updating items on the election systems would invalidate the certification of the election system by the EAC, forensic analysis revealed that after the installation of the Dominion software in August 2019, 4 EXE packages were created, 45 EXE packages were updated and/or modified, 377 Dynamic Link Libraries (DLL) were created, and 1053 Dynamic Link Libraries were modified on the EMS server. If updating the operating system with patches and updating the antivirus definition file would have invalidated the voting certification, then the county had already invalidated the certification prior to the general election of 2020. Neither security audit contracted by Maricopa County noted these findings in their report.

6.5.2.1.2 Log Management

The Cybersecurity and Infrastructure Agency (CISA) recommends that organizations should set up centralized log management systems that 1) forward logs from local hosts to a centralized log management server, correlate logs from both network and host security devices, and review both centralized and local log management policies to maximize efficiency and retain historical data. Analysis of the systems revealed that none of these recommendations were being followed on the Maricopa County election systems. In fact, in a later paragraph this report details how the windows security logs for the EMS server were in fact intentionally deleted such that the logs no longer covered the time period for the 2020 General Election. Neither security audit contracted by Maricopa County noted this finding in their report.

6.5.2.1.3 Credential Management

The Cybersecurity and Infrastructure Agency (CISA) states that Managing passwords and using strong passwords are important steps in preventing unauthorized access to databases, applications, and other election infrastructure assets. CISA further recommends that usernames be assigned to a specific person, not be shared and be changed every 90 days. CISA actually recommends that multifactor authentication be enabled for election systems. Key to the username and password concept is to be able to uniquely identify a user, assure authorized access by a given users, and to be able to hold that individual accountable for the actions performed by that assigned account. In the case of the Maricopa County election systems, none of these guidelines were followed. Neither security audit contracted by Maricopa County noted this finding in their report.

Maricopa County Failed to Ensure Unique Username Allocation to Individuals

Generic username accounts were created as part of the Dominion Software installation on 8/06/2019. These accounts were not assigned to a specific individual but appear to have been shared accounts based on function, not individual accountability. Neither security audit contracted by Maricopa County noted this finding in their report.

Maricopa County Failed to Create Unique Passwords for Each Account

Unique passwords were not created for each account. Just to be clear, the same password was used for all the accounts (if there was in fact a password for the account). This action violates every principle of password management guideline as published in every cyber security framework that currently exists. Below are the list of accounts and the corresponding password. Note the last 4 characters of the password has been masked for security reasons, but all 4 of those characters are the same for all accounts. Furthermore, these passwords had not been changed since the Dominion software suite had been installed (presumably by Dominion employees) in August of 2019. The recommendation from CISA and most cybersecurity frameworks recommend that passwords, especially for administrative accounts, should be changed every 90 days. Neither security audit contracted by Maricopa County noted this finding in their report.

Account Name	Password	Account Name	Password
[redacted]			

Account Name	Password	Account Name	Password
[redacted]			

Note: These passwords were subsequently used in conjunction with accessing virtual machines that were created from copies of the forensic images and were proven to be legitimate passwords. Neither security audit contracted by Maricopa County noted this finding in their report.

6.5.2.1.4 Lack of Baseline for Host and Network Activity

The analysis of the computing systems that comprised the Maricopa County voting system (to the extent produced) did not find any whitelisting, monitoring, baselining, or network programs that could have been used to establish a baseline for host and network activity. CISA recommends that counties leverage software and monitoring functions to establish and enforce a software and a network baseline of approved programs, communications protocols, and communications devices for voting systems. This baseline should be monitored and integrated into an alerting and response capability to ensure that no unauthorized programs are executed on the endpoints in the network and there are no unauthorized devices communicating on the network. Neither security audit contracted by Maricopa County noted this discrepancy or finding in their report.

6.5.3 Subpoenaed Equipment Not Yet Provided

Likelihood: Medium **Impact:** High

SLI Compliance report page 11 states that the Maricopa County produced 6 EMS computers. Further analysis indicated that there were 4 EMS workstations and 2 EMS servers. Maricopa County only produced 1 EMS server and 4 EMS workstations despite the Arizona Senate subpoena requesting ALL EMS servers and systems utilized in the 2020 General Election. This has impacted the ability to complete the audit of the digital network and devices. For example, if malware was resident on the missing EMS or that machine was utilized in any manner to manipulate the results of the election; this would not be able to be determined from our analysis.

6.5.3.1 Instances

6.5.3.1.1 Network Related Data

The Arizona Senate Subpoena to the Maricopa County Board of Supervisors included the production of network routers, router configuration files and managed switches used in the 2020 General Election. In subsequent conversations with county officials and county attorneys between 4/22/21 and 4/30/21 these officials agreed to provide virtual access to the systems and to provide archived Splunk data beginning 60 days prior to the election and ending 90 days following the election. Maricopa County refused to provide any data citing that the production of the router data would compromise ongoing law enforcement operations and the personally identifying information (PII) of Maricopa County residents. Maricopa County and the Arizona State Senate recently settled their dispute regarding outstanding subpoena items, so this portion of the audit is not yet complete.

6.5.3.1.2 Poll Worker Laptops

Despite the presence of at least one poll worker laptop at each voting center, the auditors did not receive laptops or forensic copies of their hard drives. It is unknown, due to the lack of this production, whether there was unauthorized access, malware present or internet access to these systems.

6.5.3.1.3 ImageCast Precinct (ICP) Administrator Credentials and Hardware Tokens

Maricopa County utilized the Dominion ImageCast Precinct 2 (ICP2) tabulator during the General 2020 election. These tabulators are normally configured with cellular wireless connections, Wi-Fi access and multiple wired LAN connections. The ICP2 actually requires two forms of authentication to configure, check and/or access the device, a numerical password and an iButton token. Maricopa County produced iButton credentials for Poll Workers to open and close polls on the ICP2's but did not produce any credentials to access the higher level administrative or configuration settings for the tabulators. This prevented the verification of the ICP2 settings to include the cellular wireless settings, the local area network settings, the wide area network settings and access to the administrative configuration reporting functions. During the course of the examination, we were able to recover the higher-level admin's numerical password from the EMS SQL Database. We also attempted to create administrative level iButton credentials utilizing the EMS system forensic images mounted in a Virtual Machine (VM) environment. The VM of the EMS system was fully functional and was used to produce poll worker iButton credentials, however, the EMS did not have the ability to create the administrative ICP2 credential.

The EMS, as produced to the auditors, only had the Poll Worker role programmed into EMS. The Poll Worker role did not have the necessary privileges and functionality to create an administrative iButton credential. In their response to the Arizona Senate request for the administrative ICP2 iButton credentials, the Maricopa County officials indicated that they did not possess these credentials and only the contracted Dominion employees have access to these credentials. Dominion has refused to comply with the production request. Given the inability to create administrative tokens with the EMS and the statement by Maricopa County concerning the ownership of the administrative iButtons, Maricopa County is unable to validate tabulator configurations and independently validate the voting system prior to an election. Additionally, since Maricopa County does not control the administrative iButtons, Maricopa County is apparently unable to independently configure, validate the voting systems prior to an election, or satisfactorily freeze the configuration of the systems for the required time periods during an election. If only the vendor controls the administrative iButtons, Maricopa County has no way of checking the configuration of the tabulators.

6.5.3.1.4 IPX and Other Devices

Based on the videos of the Maricopa County Tabulation and Election Center (MCTEC) there are a significant quantity of systems that were used in the voting process for the 2020 General Election that were not produced, including the items pictures below.

Figure 16-Video Taken on 8 November 2020 of Maricopa County ICX Systems

Figure 17-Video Capture Taken from Maricopa County Live Stream

6.5.3.1.5 Other Devices Connected to the Election Network

Examination of the network configurations for the produced systems determined that the programmed gateway for all the systems was [redacted]. This normally refers to the network router used to route network traffic external to the [redacted]. This device could also have been a managed switch. In either case, the device was not produced. The DNS cache has an entry for [redacted] with an IP address of [redacted], indicating that this system had been communicated with the EMS server and was probably used for printing. Given the naming convention of the device, [redacted], MCTEC is the acronym for the Maricopa County Tabulation and Election Center. This device has not been produced by Maricopa County. Therefore, there are additional network components that the county has not acknowledged and that are in tension with the public statements made by the county that the election system did not have any routers and was completely isolated from the internet.

[redacted]

Figure 18-DNS Update Table Recovered from the Maricopa County EMS.

Figure 19-Default Gateway Settings

6.5.4 Anonymous Logins

Likelihood: Medium **Impact:** Medium

There are common functions in Microsoft Windows that will record an anonymous login activity into the windows security logs. These logins, however, exhibit known recording sequences within the logs that allow analysts to determine the origination of the requesting function and determine the legitimacy of the logged action. An example of this behavior is the windows response to a request to access a Windows Server Message Block (SMB) share, also known as a network drive. When a user requests a connection to network drive, that initial connection request is logged as an anonymous user. The log entry also records the requestor's host name and the requestor's IP address. That anonymous request is then immediately followed up with another logged entry that authenticates the user's actual username and password in order to grant access. Below is a screen shot of this normal windows activity. Notice that the workstation name, source network IP and source port fields of this log entry contains valid data. This log entry is immediately (within one second) followed by the successful authentication of the username that is authenticating to the network drive for access permissions. That subsequent user authentication is also logged.

[redacted]

Figure 20-Normal Anonymous Request to SMB Share

While the Windows security logs from the Maricopa County EMS server only are present from 2/5/21 to 4/12/21, there are a significant number of atypical remote, anonymous logins contained in the Windows security logs. Below is an example of the atypical anonymous logons. Note that this is a remote login (login [redacted]). Note that the Workstation Name, Source Network Address and Source Port log elements are not populated, and that root/system level access is granted. It is normal for logins from the local system (login type [redacted] to not populate these data fields, but the fact that it is a network remote login (login type 3), and the fields are not populated is irregular and indicates that this is not a typical anonymous login. A search of the event logs from other Windows 2012 R2 servers did not reveal a single logon type [redacted] anonymous log entry that did not record these log data elements.

[redacted]

Figure 21-Atypical Remote Anonymous Access to EMS Server

Without access to the network data, it is impossible to determine the origin of these successful atypical remote anonymous logons. The fact that there effectively was no user account and password controls resulting in shared user accounts and passwords, coupled with the lack of network data, makes it impossible to determine if these accesses were legitimate or unauthorized without the network data. This portion of the audit is therefore not yet complete.

6.5.5 Dual Boot System Discovered

Likelihood: Medium **Impact:** Medium

Analysis of the system labeled Adjudication 2 (CyFIR evidence designation AZAud-E-087) revealed that this system contained two bootable hard drives. These two hard drives were subsequently labeled One of the AZAud-E-087-1 and AZAud-E-087-2. Neither security audit contracted by the Maricopa County noted this finding in their report.

7.5.5.1 Analysis of AZAud-E-087-1 determined the following:

[redacted]

Configured to communicate with an SMTP server address of [redacted] in the Dominion Voting Systems NLog.config file. Note: the nslog.config files on this system also contained clear text passwords, one of which was the password for the emsdbadmin account.

7.5.5.2 Analysis of AZAud-E-087-2 determined the following:

[redacted]

The discovery of a system with a dual boot configuration is a significant finding. First, it demonstrates a failure in the hardware configuration management of the Maricopa County election systems. Second, two bootable hard drives within the same system, under certain circumstances would create a situation where one operating system could act as a "jump box" where one system could access the internet and the other system would be restricted to an isolated network. This is commonly called a dual homed access and could have provided an access route into the voting system network. Without the router data, historical Splunk data and NetFlow data, we cannot complete the full analysis of the impact of this dual boot computer. Neither of the two audits performed by Maricopa County detected or reported this additional, bootable hard drive on the Adjudication 2 system.

[redacted]

6.5.6 EMS Operating System Logs Not Preserved

Likelihood: Low **Impact:** High

The Windows event logs that were present on the EMS Server that was produced by Maricopa County contain Windows security event logs ([redacted]). This file records the Windows operating security events for the EMS server including all user accesses, whether those accesses are from the local system itself or from accessing the system remotely. This log file was restricted by a policy set by Maricopa County to a file size of 20,480KB (20MB). The logging activity was set to automatically overwrite the existing log entries if the security file exceeded this size. The overwrite action would write a new log entry and delete the oldest entry in the log file. In the case of the security.evtx file on the EMS server, the earliest retained log entry was dated 2/5/2021 10:37:49 AM (the last day of the Pro V & V audit) and the latest entry was dated 4/12/2021 4:53:16 PM. The logs were not preserved and did not cover the dates for the general election (3 November 2020). An examination of the EMS and other systems involved in the 2020 General Election did not discover any enabled external log aggregation functionality nor were historical logs beyond those that were contained on the operating systems provided to the digital examination team. The security access logs were not preserved and were overwritten.

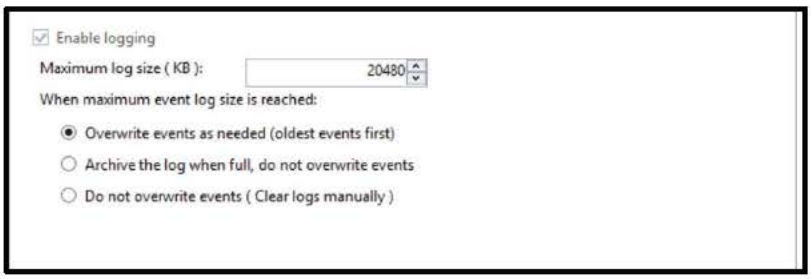


Figure 22-Policy Settings EMS Security.evtx

6.5.6.1.1 User Log Deletions on 2/11/2021

A user leveraging the emsadmin account remotely logged into the EMS server at 2/11/2021 9:08:27 AM via terminal services and began executing a script at 2/11/2021 9:09:04 AM that checked accounts for blank passwords. The event logs record this connection as originating from a system with the IPV6 address of [redacted], which is a local network IPV6 address. Between 2/11/2021 8:09:04 AM and 2/12/2021 7:12:55 AM this user ran this check 462 times. Each time the check was performed a new line was added to the security log, which had the effect of deleting the oldest entry in the log file due to the previously mentioned log size limitation setting. 462 older log entries were deleted via this method.

6.5.6.1.2 User Log Deletions on 3/03/2021

A user utilizing the emsadmin account remotely logged into the EMS server at 3/3/2021 11:12:31 AM and began executing a script at 3/3/2021 11:13:44 AM that checked accounts for blank passwords. The event logs record this connection as originating from a system with the IPV6 address of [redacted], which is a valid IPV6 local network address. Between 3/3/2021 11:12:31 AM and 3/5/2021 7:58:04 AM this user ran the script 37,686 times. Each time the check was performed a new line was added to the security log, which had the additional effect of deleting the oldest entry in the log file due to the previously mentioned log size limitation setting. 37,468 older log entries were deleted via this method.

This was 14 days after the Arizona State Senate described the risk of evidentiary loss due to continued use of election equipment, and 6 days after Judge Thomason ruled that the subpoena needed to be complied with.

Figure 23-3 Identified but Unnamed Individuals at the keyboard at 3/3/2021 at 11:06AM

6.5.6.1.3 User Log Deletions on 4/12/2021

A user utilizing the emsadmin account began executing a script at 4/12/2021 1:39:38 PM to check accounts for blank passwords. Between 4/12/2021 12:39:38 PM and 4/12/2021 12:45:13 PM this user ran this check 330 times. Each time the check was performed a new line was added to the security log, which had the additional effect of deleting the oldest entry in the log file due to the afore mentioned log size limitation setting. 330 older log entries were deleted via this method.

Figure 24- County Employee at the EMS Keyboard on 4/12/2021 at 12:39PM the time of the last blank password check was run.

7.5.5 Internet Connections

Likelihood: Medium **Impact:** Medium

The Maricopa County Board of Supervisors has repeatedly stated that the network connecting the election /voting systems is an isolated network that has no ability to connect to the internet. An in-depth analysis of both the allocated and unallocated space of the EMS, EMS workstations, Adjudication Workstations and other elements of the election system has definitively proven that this is not the case. There were hundreds of connections to public internet sites recovered from the unallocated areas of the hard drives. For the purpose of this report, only internet connection artifacts that contained valid dates after the installation of the Dominion Software suite on 8/6/2019 were included in this report. Additionally, for the purposes of this report only sites that have been visited multiple times were reported to avoid false reporting of default internet histories. Given that the Dominion Software suite was installed on 8/6/2019, no internet history URL visit dates should exist after that date.

The county did not provide a network diagram, a function diagram or any other documentation to determine if in fact a given system was supposed to be connected to the internet. Public statements by the county made clear that no election related system was connected to the internet. For the purposes of the internet examination, auditors used this statement as the starting point to prove or disprove that there was internet connectivity accessible to the systems provided by the county as a result of the subpoena. In the course of the examination definitive evidence was recovered that the EMS, EMS Client 1, EMS Client 3, EMS Client 4, REWEB 1601, and the REGIS 1202 systems had access to the internet after the installation of the Dominion voting software suite was installed on 8/6/2019. Given the nature of unallocated space analysis this is by no means a complete recovery of all internet history, but is definitive for the recovered internet artifacts on the dates and times indicated.

6.5.6.2 Internet Connections to the EMS

The EMS Server had 3 connections on 2/2/2021 to the URL [redacted]

[redacted]

6.5.6.3 Internet Connections to the EMS Client 1

The EMS Client 1 had 9 Connections to the internet between 2/7/2020 and 2/22/2021, specifically to the go.microsoft.com and www.bing.com URL's.

[redacted]

In addition to the HTTP(S) connections, there were 51 records recovered that contained 143 connections to an internal device that was not produced by Maricopa County with an IP address of [redacted].

[redacted]

6.5.6.4 INTERNET CONNECTIONS TO THE EMS CLIENT 3

The EMS Client 3 had 6 Connections to the internet to the go.microsoft.com URL.

[redacted]

6.5.6.5 INTERNET CONNECTIONS TO THE REWEB 1601 SYSTEM

The county provided what was represented as a "forensic image" of the system with the hostname [redacted]. This in fact was not an actual forensic image, but rather a copy of the hard drive on a 4TB external drive. It is unknown what actions were taken by the County to ensure that the drive was wiped prior to the system copy. A carve for internet history artifacts recovered 890 internet records, each with multiple visit iterations for public URL connections including foxnews.com, maricopa.gov, Microsoft.com, msn.com and adnxs.com.

[redacted]

6.5.6.6 Internet Connections to the REGIS 1202 System

The county provided what was represented as a “forensic image” of the system with the hostname REGIS 1202. This in fact was not an actual forensic image, but rather a copy of the hard drive on a 4TB external drive. It is unknown what actions were taken by the County to ensure that the drive was wiped prior to the system copy. A carve for internet history artifacts recovered 205 internet records, each with multiple visit iterations for public URL connections including maricopa.gov, Microsoft.com, and logons to the localhost.

[redacted]

7.6 Low Findings

7.6.1 Election Data found From Other States

Likelihood: Low **Impact:** Medium

The Maricopa County Adjudication 2 system had two bootable hard drives. The drive identified as [redacted] contains a directory [redacted]. Inside of that directory are subdirectories that appear to contain data from other jurisdictions and what appears to be demonstration data. Specifically, these directories are named [redacted]. One can reasonably assume that WA is an abbreviation for Washington and SC is an abbreviation for South Carolina. There is no known need for this external data to be located on a Maricopa County adjudication system. Neither of the two audits performed by Maricopa County reported this finding.

[redacted]

Figure 26-General with Variable SP Directory

Figure 27-SC Cert Cookie General Directory Structure

[redacted]

Figure 29-Special Election with Fusion Directory

[redacted]

Figure 28 - WA Cert General 2018 vA Directory

7 About Cyber Ninjas

Cyber Ninjas is an application security consulting company specializing in ethical hacking, training, and security program development. Our staff represents over 10 years of experience in a variety of areas including application support, development, product management, and application security. This experience across all areas of the software development life cycle gives us a unique perspective on how to build security into your existing processes. With everything we do, our goal is to build the knowledge within your organization. We strongly believe that "Security comes with knowledge," and that it is our job as Cyber Ninjas to train and teach through every engagement to build up capabilities within your organization.

EXHIBIT 21

A. V. Shiva Ayyadurai, Ph.D., Pattern Recognition Classification of Early Voting Ballot (EVB) Return Envelope Images for Signature Presence Detection: An Engineering Systems Approach to Identify Anomalies to Advance the Integrity of US. Election (Sept. 2124, 2021)

Pattern Recognition Classification of Early Voting Ballot (EVB) Return Envelope Images for Signature Presence Detection

An Engineering Systems Approach to Identify Anomalies to Advance the Integrity of U.S. Election Processes

AUTHOR
Dr. Shiva Ayyadurai, MIT PhD
SMVS, SMME, SBEE
701 Concord Avenue
Cambridge, MA 02138

FINAL REPORT
SEPTEMBER 24, 2021

PREPARED FOR

Honorable Senator Karen Fann
President of the Senate
Arizona State Senate
1700 West Washington Street
Phoenix, AZ 85007

© 2021. Dr. Shiva Ayyadurai.

EchoMail, Inc.
701 Concord Avenue
Cambridge, MA 02138 U.S.A.
Phone: 617-631-6874
Email: vashiva@echomail.com

SEPTEMBER 2021

ECHOMAIL AZ092021-1

Pattern Recognition Classification of Early Voting Ballot (EVB) Return Envelope Images for Signature Presence Detection

An Engineering Systems Approach to Identify Anomalies to Advance the Integrity of U.S. Election Processes

AUTHOR
Dr. Shiva Ayyadurai, MIT PhD
SMVS, SMME, SBEE
701 Concord Avenue
Cambridge, MA 02138
vashiva@echomail.com
617-631-6874

FINAL REPORT
SEPTEMBER 24, 2021

PREPARED FOR

Honorable Senator Karen Fann
President of the Senate
Arizona State Senate
1700 West Washington Street
Phoenix, AZ 85007

EchoMail, Inc. Proprietary and Confidential

DEDICATION

To the American People
Beyond Left & Right
Who Seek Truth Freedom Health

EchoMail, Inc. Proprietary and Confidential.

TABLE OF CONTENTS

Acknowledgements – 6
Author's Bio – 7

ABSTRACT – 9
SUMMARY RESULTS – 13
KEY FINDINGS – 14

INTRODUCTION – 17
ENGINEERING SYSTEMS APPROACH – 18
EVB SYSTEMS PROCESS – 21
Signature Presence Detection – 22
Signature Verification – 23
MARICOPA EVB RESULTS SUMMARY – 29
SCOPE OF AUDIT – 32

METHODOLOGY - 34
FOUNDATIONS OF PATTERN RECOGNITION– 34
PATTERN RECOGNITION EXAMPLES – 39
MATHEMATICAL MODELING – 47
SIGNATURE/SIGNAL DETECTION AND CLASSIFICATION – 49
EVB RETURN ENVELOPE IMAGE CLASSIFICATION – 51
DATA SET OF EVB RETURN ENVELOPE IMAGES - 52
ECHOMAIL EVB SIGNATURE PRESENCE DETECTION SYSTEM – 58

RESULTS - 61
EVB RETURN ENVELOPE IMAGES COUNT – 61
DUPLICATES ANALYSIS - 62
UNIQUE EVB RETURN ENVELOPE IMAGES - 62
DUPLICATE IMAGE EXAMPLES – 63
SIGNATURE PRESENCE DETECTION RESULTS – 67
SUMMARY OF ECHOMAIL ANALYSIS – 70
EVB RETURN ENVELOPE IMAGES OF SCRIBBLES AND BLANKS – 70
GLOBAL TEMPORAL SIGNALS ANALYSIS – 72
SUPERVISED IMAGE REVIEW – 77

DISCUSSSION - 87
COMPARATIVE ANALYSIS - 87
QUESTIONS FOR MARICOPA ELECTION OFFICIALS - 91
FUTURE RESEARCH – 93

CONCLUSION - 96

ACKNOWLEDGMENTS

Special thanks to the leadership of the Arizona State Senate, the many stakeholders, and the engineering team at EchoMail for their hard work and sincere efforts.

AUTHOR'S BIO

Dr. Shiva Ayyadurai, MIT PHD, SMME, SMVS, SBEE, the inventor of email and polymath, holds four degrees from MIT, is a world-renowned engineer, systems scientist, inventor and entrepreneur. He is a Fulbright Scholar, Lemelson-MIT Awards Finalist, India's First Outstanding Scientist and Technologist of Indian Origin, Westinghouse Science Talent Honors Award recipient, and a nominee for the U.S. National Medal of Technology and Innovation. He holds multiple patents, is the author of twenty books, and has published original research, in leading peer-reviewed high-impact scientific journals including *IEEE, IJPRAI, Nature Neuroscience, CELL Biophysical Journal,* that have received thousands of citations. He has started seven successful high-tech companies, received numerous industry awards, consults for Global 2000 organizations and government, and has been invited to present Keynote and Distinguished lectures at leading institutions such as NSF, NIH, FDA, Harvard, and at MIT, where he delivered the Presidential Fellows Lecture.[1]

In 1978, as a 14-year-old, he was recruited as a Research Fellow by the University of Medicine and Dentistry of New Jersey (UMDNJ), in Newark, NJ after graduating with Honors from a special program in Computer Science at the Courant Institute of Mathematical Science at NYU. At UMDNJ, he invented email – ***the system*** as we know it today – when he was the first to convert the old-fashioned *interoffice paper-based mail system* consisting of the Inbox, Outbox, Memo (To:, From:, Date:, Subject:, Cc:, Bcc:), Attachments, Folders, etc. into its electronic equivalent by writing 50,000 lines of code to create a software system, which he named "Email," – a term never used before in the English language – and went on to be awarded the first U.S. Copyright *TXu 111-775* for "EMAIL, COMPUTER PROGRAM FOR ELECTRONIC MAIL SYSTEM" recognizing him as the inventor of email at a time when Copyright was the only legal mechanism to protect software inventions. Only in 1994 did the Federal Circuit recognize software as a "digital machine" allowing for software patents. Email is not the simple exchange of text messages. Dr. Shiva has never claimed to be the inventor of electronic messaging, which predates email - the system that he created in 1978.[2,3]

Recognizing his talents in software programming, UMDNJ gave him the opportunity to conduct medical research focused on developing pattern recognition classification methods for categorization of sleep signature patterns from babies with Sudden Infant Death Syndrome (SIDS). His research was published in IEEE and presented at the IEEE-EMBS conference in Espoo, Finland. Since that time and for more than forty years, his research and development efforts in academia and industry have been focused in the field of pattern recognition classification systems, systems science, and development of large-scale computational systems for analysis of diverse signals and signatures across a range of industries: biology and

[1] Dr. Shiva Ayyadurai, Biography and Curriculum Vitae, https://vashiva.com/about-va-shiva-ayyadurai/

[2] Facts on the invention of email, https://www.inventorofemail.com/thefacts/

[3] The Man Who Invented Email, TIME, https://techland.time.com/2011/11/15/the-man-who-invented-email/

medicine, engineering (e.g. aeronautical, civil, mechanical, electrical), banking, finance, and, government, as well as across a diversity of applications including handwriting recognition of courtesy amounts on bank checks, automatic analysis and classification of electronic documents e.g. email, ultrasonic and radar wave signature classification for non-destructive evaluation (NDE), signals analysis of Tadoma feature identification, biomarker analysis for determining signatures of efficacy for multi-combination therapies, image analysis for cardiology, and signal detection of fluid flow anomalies in fluidized bed reactors.

He earned a Bachelors in Electrical Engineering and Computer Science, a Masters in Mechanical Engineering, and another Masters in Visual Studies from the MIT Media Laboratory. In the midst of his PhD research in 1993, where he aimed to create a generalized platform – *Information Cybernetics* – for pattern recognition, he won an industry-wide competition sponsored by the White House, Executive Office of the President, to automatically analyze and classify President Clinton's email, resulting in his developing EchoMail® - a platform for automatic classification of electronic documents –, and subsequently launching EchoMail, Inc., a company that grew to nearly $200 million in market valuation. EchoMail today applies its technologies across a diversity of applications.

In 2003, he returned to MIT complete his doctoral work in systems biology in the department of Biological Engineering where he developed CytoSolve®, a scalable computational systems biology platform for mathematically modeling the whole cell. Following his PhD, Dr. Shiva was selected for a Fulbright Fellowship returning him to India where he discovered the systems theoretic basis of eastern systems of medicine resulting in Systems Health®, a new educational program that provides a scientific foundation for integrative medicine. In 2012, Dr. Shiva launched CytoSolve, Inc. with the aim of modeling complex diseases and biomolecular processes to discover multi-combination medicines. His efforts led to CytoSolve earning an FDA allowance for a multi-combination therapy for pancreatic cancer in a record eleven months, developing innovative nutraceutical products, and garnering numerous industry and academic partnerships.

As an educator dedicated to the field of systems science and systems thinking, Dr. Shiva pioneered *Systems Visualization*, a course he taught at MIT to graduate and undergraduate students, which integrated systems theory, narrative story telling, metaphors, and data science to provide a pedagogy for visualization of complex systems. He founded the International Center for Integrative Systems, a research and educational institution and home to Innovation Corps and R.A.W./C.L.E.A.N. Food Certified, for broader applications of systems science.

Dr. Shiva has appeared in *The MIT Technology Review*, *TIME, The Wall Street Journal*, *New York Times*, *NBC News*, *USA Today* and other major media. Dr. Shiva was named Top 40 Under 40 in the *Improper Bostonian*. He continues his passion for entrepreneurialism as Managing Director of General Interactive to incubate, mentor and fund new startups in various areas including healthcare, media, biotechnology, information technology, to name a few.

Dr. Shiva is a member of Sigma-Xi, Eta Kappa Nu, and Tau Beta Pi.

Pattern Recognition Classification of Early Voting Ballot (EVB) Return Envelope Images for Signature Presence Detection

An Engineering Systems Approach to Identify Anomalies to Advance the Integrity of U.S. Election Processes

Dr. Shiva Ayyadurai, MIT PhD, SBEE, SMVS, SMME
701 Concord Avenue | Cambridge, MA 02138 | U.S.A.
Email: vashiva@echomail.com | Tel: 617-631-6874

ABSTRACT

The processing of Early Voting Ballots (EVBs), and, more broadly, election voting systems are complex *engineering systems* – sociotechnical systems – involving parallel and sequenced processes across multiple systems of systems, interconnecting diverse stakeholders.[4] Such engineering systems advance through constant observation and feedback, and particularly in response to anomalous behavior. The integrity of such engineering systems relies on a culture fostering the encouragement of stakeholders' to provide feedback and a commitment by leadership to investigate anomalies – small or large, insignificant or monumental. Engineers welcome signals of anomalous behavior for they provide a gateway to identify and resolve root cause issues towards greater systems integrity. In Maricopa County, Arizona, election officials processed 91.67% of all ballots cast in the November 2020 general election through EVB systems, as reported in the November General Election CANVASS report.[5] Constituent concerns about the 2020 U.S. general election in Maricopa County ("Maricopa") were one of the motivations for the Arizona State Senate to conduct a comprehensive audit.

[4] Early Voting Ballots (EVBs) are a method of voting prior to ("early" to) Election Day.
[5] https://recorder maricopa.gov/pdf/11-03-2020-0 Canvass BOS SUMMARY NOV2020-two-sided print.pdf, accessed September 15,2021.

This audit sought to review the count of signatures on EVB return envelopes as reported in the *CANVASS* report. The Arizona State Senate commissioned this author – Dr. Shiva Ayyadurai – based on their review of his engineering experience and his more than forty years of contributions to the field of pattern recognition classification methods and engineering systems science, to provide his expertise and EchoMail, Inc.'s capabilities to audit Maricopa's EVB return envelope images from the 2020 general election. An example of an EVB return envelope image, ***and the explicit area in which the voter must SIGN WITHIN THE BOX, ("Signature Region")***, is illustrated in Figure 1, below.

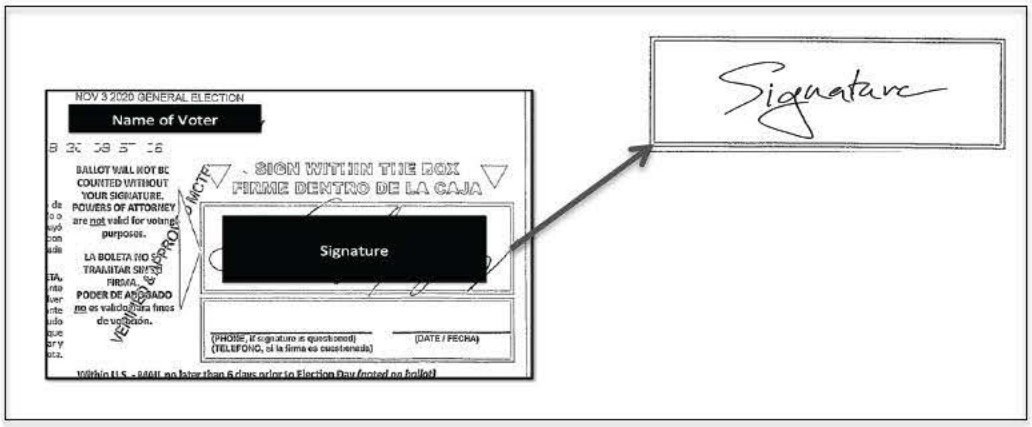


Figure 1: Example of an image of an Early Voting Ballot (EVB) return envelope, and the Signature Region, in which the voter must provide their signature.

In this audit, EchoMail was tasked with executing pattern recognition classification methods to identify the Signature Region on the EVB return envelope image, as shown in Figure 1, and then to classify that specific Signature Region as "Blank," "Likely Blank," "Scribble," or "Signature."[6] EchoMail received 1,929,240 EVB return envelope images from the Arizona State Senate that were represented to EchoMail as all EVB return

[6] A Signature Region is classified based on non-white pixel densities in the Signature Region as follows: if 0% then Blank; if 0%+ to 0.1% then Likely Blank; if 0.1%+ to 1% then Scribble; and, if greater than 1%, then as Signature. EchoMail's scope was ***not*** to identify a signature if it appeared elsewhere on the EVB return envelope image.

envelopes received by Maricopa for the November 2020 Election. EchoMail executed an array of pattern recognition classification algorithms to extract the specific Signature Region from the EVB return envelope image. The count of Signature Regions classified as Signature, was compared with the count, as reported by Maricopa election officials in the *CANVASS* report.

The analysis revealed various anomalies such as: 34,448 EVB return envelope images that were 2-Copy, 3-Copy and 4-Copy duplicates ("Duplicates") originating from 17,126 unique voters while no Duplicates were reported in Maricopa's *CANVASS* report; 6,545 ***more*** unique EVB return envelopes reported by Maricopa than that by EchoMail; 9,589 ***more*** EVB return envelopes with signatures in Maricopa's count; and, Maricopa's count of 587 "Bad Signatures" – equaling 0.031% of all EVB return envelopes received by Maricopa – appear to be surprisingly low, given that EchoMail itself, though not commissioned to audit or perform Signature Verification, detected 2,580 non-signature Scribbles, in the Signature Region, which would exceed Maricopa's "Bad Signatures" percentage of 0.031%, by over four times.

The anomalies identified in this audit raise questions on the integrity of Maricopa's EVB systems processes and support the need for further investigation including a review of Maricopa's Standard Operating Procedure (SOP) for EVB processing, Chain of Custody, and Signature Verification methods, including the methodologies for curing questionable signatures. Moreover, an independent scientific analysis of Maricopa's Signature Verification process that involves comparing *all* signatures on EVB return envelopes with the voter registration signatures is warranted. Such an effort will provide a quantitative metric to assess the confidence level of Maricopa's Signature Verification process; and,

more importantly, serve as a valuable case study towards building objective metrics to assess the entire EVB systems process. This audit, based on an engineering systems approach, and the anomalies discovered herein provide the *systems feedback* necessary for all stakeholders to advance the systems integrity of U.S. elections processes.

SUMMARY RESULTS

	EchoMail Analysis	Maricopa Reported	Variance
EVB Return Envelopes Received	**1,929,240***	***Unknown***	**NA**
Duplicate Analysis			
Duplicates[7]	(17,322)	*Un-reported*	NA
Unique EVB Return Envelopes	**1,911,918**	**1,918,463****	**(6,545)**
Signature Presence Detection			
No Signature Ballots[8]	(1,919)	(1,455)	(464)
Scribbles[9]	(2,580)	NA	(2580)
EVBs Ready for Signature Verification	**1,907,419**	**1,917,008**	**(9,589)**
Signature Verification			
"Bad Signatures"	NA	(587)	NA
"Late Returns"	NA	(934)	NA
Total EVBs Verified and Counted	**NA**	**1,915,487**	**NA**

Table 1: Summary report of EchoMail Analysis of EVB return envelope images compared with Maricopa's results reported in November General Election *CANVASS* report.

*This count is the total count of all the EVB return envelope images received by EchoMail from Arizona State Senate.

**This count is all EVB return envelopes verified and counted by Maricopa (1,915,487) plus those classified by Maricopa as "No Signatures" (1455), "Bad Signatures" (587), and "Late Returns" (934), as documented in Maricopa County's November 2020 *CANVASS* report.

[7] In the EchoMail Analysis, those EVB return envelope images with same image file name were deemed "Duplicates." The EVB return envelope image file names are voter specific. 17,126 unique voters submitted 34,448 2-Copy, 3-Copy, 4-Copy Duplicates. The *CANVASS* report filed by Maricopa election officials did not report Duplicates.

[8] "No Signature Ballots" in EchoMail Analysis are those Signature Regions on EVB return envelope images classified to be "Blanks" based on a non-white pixel density of 0%, and "Likely Blanks" based on a non-white pixel density between 0%+ to 0.1%.

[9] "Scribbles" in EchoMail Analysis are those EVB return envelope images containing likely illegible signatures in the Signature Region, wherein a scribble is defined as a Signature Region containing a non-white pixel density between 0.1%+ to 1%.

KEY FINDINGS

- **It is unknown, per the *CANVASS* report, how many EVB return envelopes were *originally* received by Maricopa election officials.** EchoMail received a data set of 1,929,240 EVB return envelope images that were represented to EchoMail as being the set of *all* EVB return envelopes originally received by Maricopa. However, the *CANVASS* report does not document how many EVB return envelopes were originally received Maricopa election officials.[10]

- **EchoMail identified 34,448 EVB return envelope images being 2-copy, 3-copy and 4-copy Duplicates** originating from 17,126 unique voters, while no Duplicates were reported in Maricopa's *CANVASS* report.[11]

- 6,545 ***more*** unique EVB return envelopes were processed by Maricopa than identified by EchoMail.

- 464 ***more*** "No Signature" EVB return envelopes were reported by EchoMail. EchoMail identified 1,919 EVB return envelope images with Blank or Likely Blank in the Signature Region i.e. "No Signature." Maricopa reported 1,455 "No Signature" EVB return envelopes.

- 2,580 Scribbles identified by EchoMail in the Signature Region of EVB return envelope images. A "Scribble" is when a Signature Region on an EVB return

[10]All EVBs reported that were received by Maricopa are assumed to have been accompanied by return envelopes or affidavits with signatures.
[11]The 2020 November General Election *CANVASS* report does not mention Duplicates. A search of the keyword "duplicate" reveals no instances in the *CANVASS* report.

envelope image contains a non-white pixel density between 0.1%+ to 1%, and may indicate a potential "Bad Signature." EchoMail was not commissioned with the task of performing Signature Verification.

- Maricopa reported 587 "Bad Signatures," which is 0.031% of the total EVB return envelopes received by Maricopa. Though EchoMail was not commissioned to perform Signature Verification, if EchoMail's identification of 2,580 Scribbles were all designated as "Bad Signatures," that would be 0.134% of Maricopa's total EVB return envelopes received. This percentage is at least four times more than the "Bad Signatures" percentage reported by Maricopa.

- While the number of EVB returns envelopes in Maricopa for the 2016 general election ***increased*** from 1,257,179 to 1,918,463 EVB return envelopes for the 2020 general election, representing a 52.6% ***increase*** (or by 661,284 EVB return envelopes), the number of rejections from Signature Mismatches of EVB return envelopes, from 2016 to 2020, ***decreased*** by 59.7%. This inverse relationship requires explanation.

- 9,589 ***more*** EVB return envelopes were submitted for Signature Verification by Maricopa than the EVB return envelope images identified by EchoMail as having signatures.

- A full audit of Maricopa's Signature Verification process is necessary, and can be accomplished by comparing each signature on EVB return envelope images with an

image of the voter's signature from voter registration files. This will provide a quantitative metric to assess confidence level of Signature Verification.

- Disclosure of Maricopa's Standard Operating Procedure (SOP) for EVB processing, Chain of Custody, and Signature Verification methods, including the SOP and methodology for curing questionable signatures, is necessary.

INTRODUCTION

The 21st century is the era of complex *engineering systems*.

The processing of Early Voting Ballots (EVBs), and, more broadly, election voting systems are complex engineering systems – sociotechnical systems – involving parallel and sequenced processes across multiple systems of systems, interconnecting diverse stakeholders.[12] Early Voting Ballots (EVBs) are a method of voting prior to i.e. "early" to, Election Day. In Maricopa County, Arizona, election officials processed 91.67% of all ballots cast in the November 2020 general election through EVB systems as reported in the November General Election CANVASS report.[13]

Over the past two decades, the nascent discipline of engineering systems has evolved towards developing a systems theoretic framework, including new pedagogies and *lingua franca*, to comprehend the complexity of large-scale systems involving multiple stakeholders. These developments are essential to build and deliver systems that meet stakeholders' implicit and explicit needs. Engineering systems recognize that the needs of stakeholders – voters, in this case – can best be addressed through a sociotechnical systems approach in defining the properties of such systems.

[12] Early Voting Ballots (EVBs) are a method of voting prior to ("early" to) Election Day.
[13] https://recorder maricopa.gov/pdf/11-03-2020-0 Canvass BOS SUMMARY NOV2020-two-sided print.pdf, accessed September 15,2021.

ENGINEERING SYSTEMS APPROACH

The modern world has moved from the world of creating simple isolated components to a world of tightly coupled systems of systems. The engineering systems approach offers a framework to study such systems. While the goals of this audit are well defined, this manuscript also aims is to motivate an engineering systems perspective in election voting systems with the hope of moving beyond partisanship, vitriol, and controversy, to appreciate that modern election voting systems are indeed complex engineering systems.

In the fields of global manufacturing and supply chains, transportation systems, space travel and aeronautical systems, electrical power generation and distribution networks, self-driving autonomous vehicle management systems, and modern health care systems, that appreciation has emerged. Stakeholders of election voting systems: election officials, voters, suppliers, and policy makers may greatly benefit from such a concomitant appreciation to advance the integrity of a foundational system that aims to enable a democracy for a wide range of stakeholders, beyond left and right.

Such engineering systems advance through constant observation and feedback, and particularly in response to anomalous behavior. The integrity of such engineering systems relies on a culture fostering stakeholders' encouragement to provide feedback and a commitment to investigate observed anomalous behavior – small or large, insignificant or monumental. Engineers welcome signals of anomalous behavior for they provide a

gateway to identify and resolve root cause issues towards greater systems integrity. Constituent concerns about the 2020 U.S. general election in Maricopa County was one of the motivations for the Arizona State Senate to conduct a comprehensive audit.

One element of this audit sought to review the count of signatures on EVB return envelopes as reported in the *CANVASS* report. The Arizona State Senate commissioned this author – Dr. Shiva Ayyadurai – based on their review of his engineering experience and his more than forty years of expertise in the field of pattern recognition classification methods and engineering systems science, to provide his and EchoMail, Inc.'s capabilities to audit Maricopa's EVB return envelope images from the 2020 general election.

Identifying and addressing root causes of such anomalies can only lead to one outcome: a more robust election system exhibiting the properties of precision, reliability, auditability, and reproducibility, among others. Over the past two decades, engineering systems theory and pedagogies have developed the *lingua franca* of such properties or "ilities," in order to define requirements of a system that can have overall impact on system behavior; for example, the top twenty "ilities" are identified in the graph in Figure 2 below.[14] The "ilities" in this graph are based on an analysis of journal articles and google hits of many well-known and common engineering systems. The top four "ilities" are quality, reliability, safety, and flexibility.

[14] p.67, http://strategic.mit.edu/docs/es_book_004_proof.pdf accessed on September 15, 2021.

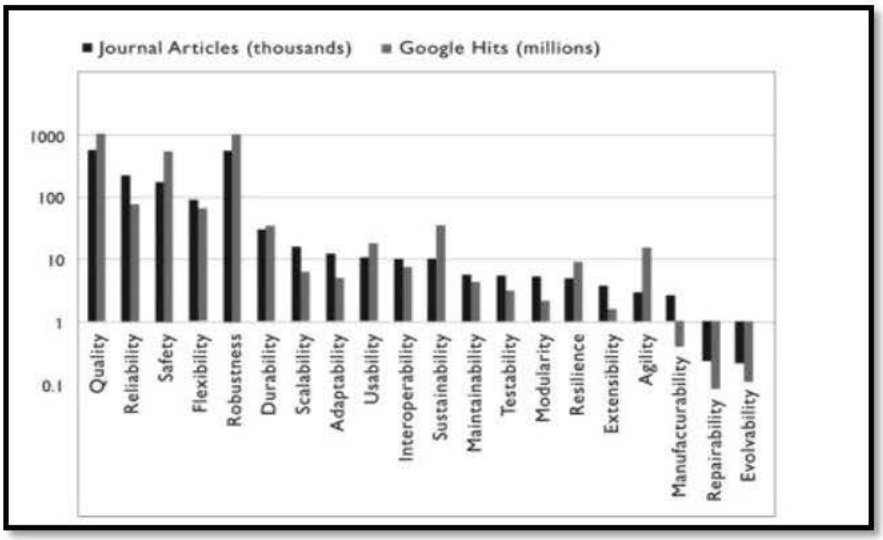


Figure 2: The Top 20 "Ilities"[8]

When considering election voting systems, given the interconnectivity of such systems with the most important stakeholders – voters –, while reliability emerges as an obvious desirable systems property, other "ilities" such as, precision (does not have to end in "ility"), auditability, and reproducibility of election results, for example, though not identified in the above graph, are likely to be some of the most relevant and necessary properties for ensuring integrity in election voting systems. The non-existence of these key "ilities" in the above graph reflects the likely reality that engineering systems approaches to election voting systems are a relatively new application area. The efforts herein, therefore, provide a unique and historic opportunity for an engineering systems approach to election voting systems.

THE EVB SYSTEMS PROCESS

The processing of Early Vote Ballots (EVBs) is a multi-step engineering systems process requiring many "ilities" (properties that have yet to be perhaps consciously decided by all stakeholders) such as precision, reliability, auditability, and reproducibility.

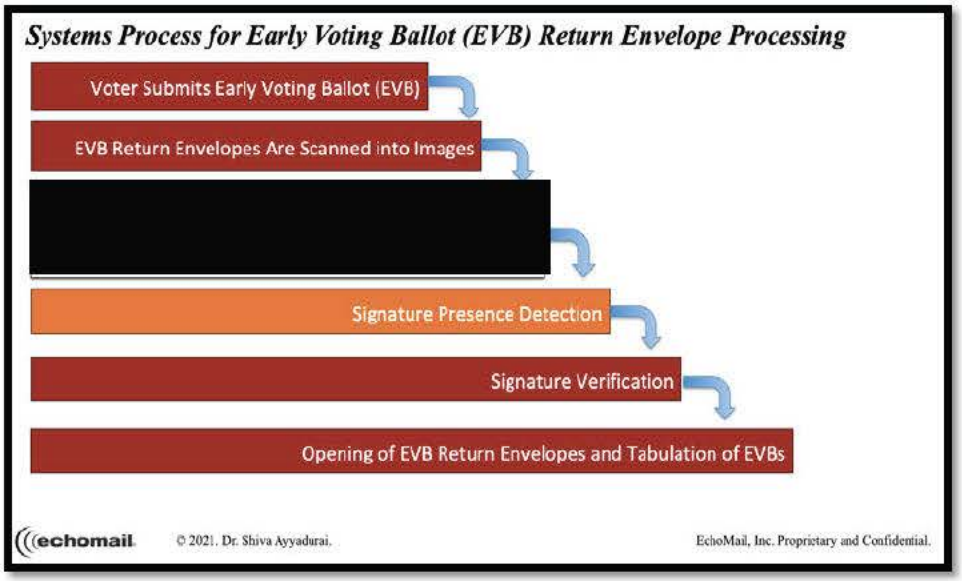


Figure 3: The systems process for Early Voting Ballot (EVB) return envelope processing.

Figure 3 provides the key steps in the multi-step systems process of EVBs. After a voter submits their EVB in a return envelope, the EVB return envelopes are scanned into digital images. EVB return envelopes come in an assortment of formats depending on location, and voter needs. There are EVB return envelopes for U.S. citizens residing in the United States, for those residing outside of the United States, and as well for military personnel. In addition, formats vary for those with poor eyesight e.g. large print format, and the blind e.g. Braille format. The images are stored in file types such TIFF and PDF.

One of the critical steps in the processing of EVBs is to ensure the *presence* of a signature. Voters are expected to sign their names in a specific Signature Region on the envelopes or affidavit accompanying the EVB. ***The instructions indicate that the voter must sign inside the box. Per the Scope of Audit, EchoMail is to analyze, solely this Signature Region.***

Signature Presence Detection

This process of verifying a signature's existence in the Signature Region of the EVB return envelope image, is denoted as "Signature Presence Detection." Figure 4 below illustrates the key aspects of Signature Presence Detection.

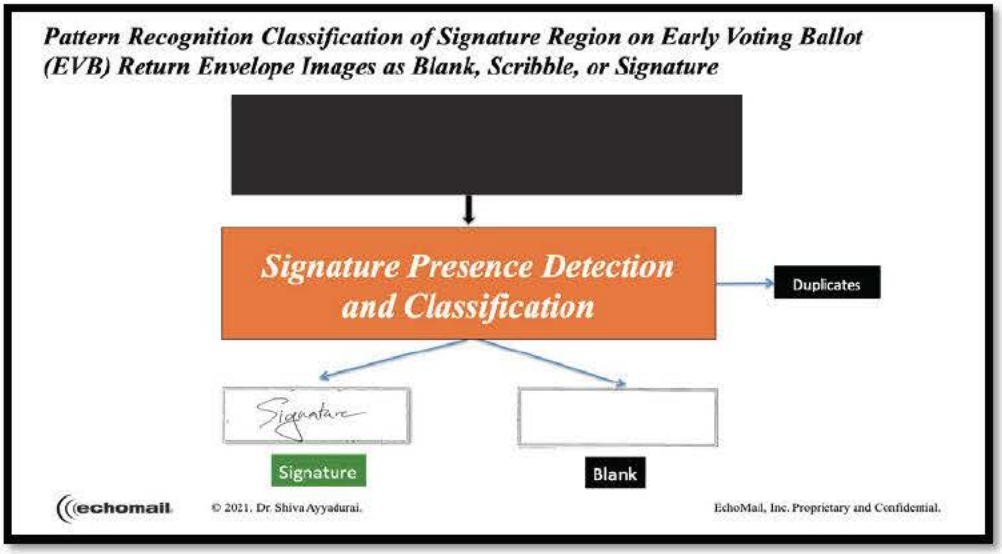


Figure 4: The key aspects of Signature Presence Detection.

The first step in this process is to receive and organize all of EVB return envelope images for classification. Another step is to tag and resolve Duplicates, so only one EVB return

envelope is associated with one unique voter i.e. "One Person, One Vote." Classification involves looking at the Signature Region and determining if it is has a Signature or a Blank i.e. "No Signature." A blank in the Signature Region is officially tagged as "No Signature." In this audit, EchoMail was tasked with further refining the classification of the Signature Region into: Signature, Blank, Likely Blank, and Scribble, which are discussed in detail in the *Scope of Audit* and *Methodology* sections.

Signature Verification

One of the other critical steps in the processing of EVB return envelopes is to verify that the signature in the Signature Region matches with signature that the election officials have on file for the voter. This process denoted as "Signature Verification" appears to vary from state to state, and even from county to county. During Signature Verification, the reviewer may also look for a signature elsewhere, beyond the Signature Region, on the EVB return envelope. Information from the Recorder's office in Maricopa along with information provided by an independent organization's interview with Maricopa election officials reveals the key elements of Signature Verification.[15,16]

Based on these information sources, and in the absence of access to a formal Standard

[15] FAQ 11 of https://recorder maricopa.gov/site/faq.aspx, accessed on September 15, 2021.
[16] pp. 13-14 of https://healthyelections.org/sites/default/files/2020-11/arizona-110220.pdf, accessed on September 15, 2021.

Operating Procedure (SOP) for Signature Verification, the process of Signature Verification appears to consist of the following elements:

- Each EVB return envelope, containing a code unique to the voter, is made available to reviewers
- The signature on EVB return envelope is reviewed by a County employee.
- During the review, the reviewers "…are trained to look at 27 different points of comparison on a signature to complete verification, including slopes, pen drops, and other identifiable components of a person's handwriting" with a signature on file that is associated with their voter registration signature, accessible using the code unique to the voter.
- Two watchers customarily observe review of signatures on EVB return envelopes – one selected from Democratic Party, and the other selected from the Republican Party.
- If the signature matches the records, the EVB return envelope is marked as "Good Signature" and the EVB is sent for vote tabulation.
- If the signature does not match, as confirmed by a second and third round of review, election officials make reasonable efforts to contact the voter and "cure" the questionable signature where "…the county recorder or other officer in charge of elections shall make reasonable efforts to contact the voter, advise the voter of

the inconsistent signature and allow the voter to correct or the county to confirm the inconsistent signature."[17]

- If unable to contact the voter and verify e.g. cure the questionable signature, the signature is not counted and the EVB is deemed to be a "Bad Signature."
- If the Signature Region of the EVB return envelope is blank, then the reviewers may look for signatures elsewhere on the EVB return envelope e.g. in the phone area, and may attempt to verify and cure. If the signature does not exist anywhere, the EVB is deemed a "No Signature."
- Any EVBs that are submitted after the deadline are classified as "Late Returns."

Table 1 displays the signature-matching practices and requirements for mail-in ballots in the battleground states.

Table 1: Legal Framework for Signature Verification in Battleground States

Battleground State	Requires Signature Verificatio a Process?	Signature Verification Practices Codified?	Witness Reqeirements?	Allows Cure of Missing Voter Signature?	Allows Cure of Mismatched Signature?	Allows Cure of Witness Signature Error?	Voters have a chance to cure signature issues *after* Election Day?
AZ	YES	YES	NO	YES	YES	N/A	YES
FL	YES	YES	NO	YES	YES	N/A	YES
MI	YES	NO	NO	YES	YES*	N/A	NO
NC**	NO	N/A	YES	YES	N/A	YES	YES
PA	NO	N/A	NO	YES	N/A	N/A	NO
WI	NO	N/A	YES	YES	N/A	YES	NO

Table 1 is color-coded based on whether or not the practice in question makes it easier (green) or harder (red) for voters to cast their ballots.

*Voters must spoil the ballot with the mismatched signature and request a new ballot. Some jurisdictions may allow voters to cure their original ballot, but there is no state law to that effect.

**Under new NCSBE Guidance issued on October 4, 2020, North Carolina's notice and cure process for missing signatures and witness defects is temporarily suspended until several pending lawsuits are resolved, likely in the near future.

Figure 5: Legal framework assessment of Signature Verification in six 2020 battleground states.[18]

In Figure 5, is a screenshot of a table from a report aggregating metrics defining the legal

[17] https://www.azleg.gov/ars/16/00550.htm, accessed September 15, 2021.

[18] p.8, http://healthyelections.org/sites/default/files/2020-10/Signature%20Verification%20Report%20(Oct%207%2C%202020).pdf, accessed September 15, 2021.

framework for Signature Verification in six battleground states in the 2020 election. This table indicates that Arizona and Florida may have the most comprehensive support for Signature Verification, as denoted by achieving five "YES" qualifications out of the seven criteria.[19] In that same report, the results of the Election Administration and Voting Survey (EAVS) of Mail-In ballot rejections for Signature Mismatch, following Signature Verification, are provided for the 2016 and 2018 general elections and midterms, respectively. In Figure 6, an extract of a table from that report, highlighting the Signature Mismatch data for the **State of Arizona**, is shown.

Table 4: Historic Ballot Rejections for Signature Mismatch (2016 & 2018 EAVS data) & Which States Are Required to Compare Signatures in the 2020 General Election

General Election: November 8, 2016					Midterm Election: November 6, 2018					2020 General
State	Rejected for Signature Mismatch	Mail-in Ballots Received	% of Votes that are Mail-in	Signature Mismatch Rejection Rate*	State	Rejected for Signature Mismatch	Mail-in Ballots Received	% of Votes that are Mail-in	Signature Mismatch Rejection Rate*	State Signature Matching Requirement?
AK	N/A	27,626	8.55%	N/A	AK	N/A	24,425	8.50%	N/A	No
AL	N/A	88,601	4.15%	N/A	AL	N/A	57,832	3.36%	N/A	No
AR	94	27,525	2.63%	0.34%	AR	21	15,208	1.92%	0.14%	Yes
AZ	2,657	2,017,722	74.11%	0.13%	AZ	1,516	1,899,240	78.81%	0.08%	Yes
CA	25,965	8,511,992	58.26%	0.31%	CA	16,116	8,286,228	59.92%	0.19%	Yes
CO	16,149	2,654,993	92.05%	0.61%	CO	13,027	2,449,409	94.70%	0.53%	Yes
CT	N/A	132,012	7.88%	N/A	CT	N/A	91,602	6.44%	N/A	No
DC	Data not available	16,625	5.33%	N/A	DC	44	9,351	4.04%	0.47%	Yes

Figure 6: Highlighting the Signature Mismatch metrics for the **State of Arizona** 2016 and 2018 general election and midterm election, respectively.

On the left side of Figure 6, for the State of Arizona for the 2016 general election, the number of Mail-In ballots received is 2,017,722; 2,657 Mail-In ballots were rejected for

[19] p.8, https://healthyelections.org/sites/default/files/2020-10/Signature%20Verification%20Report%20(Oct%207%2C%202020).pdf, accessed September 15, 2021.

Signature Mismatch, representing a Signature Mismatch Rejection Rate of 0.132%. The Signature Mismatch Rejection Rate is calculated by dividing the Mail-In ballots rejected for Signature Mismatch by the total number of Mail-In ballots received. On the right side of Figure 6, for the State of Arizona for the 2018 midterm election, the number of Mail-In ballots received is 1,899,240; 1,516 Mail-In ballots were rejected for Signature Mismatch, representing a Signature Mismatch Rejection Rate of 0.079%. These results are consolidated in Table 2.

	State of Arizona 2016 General Election	State of Arizona 2018 Midterm Election
Mail-In Ballots	2,017,722	1,899,240
Rejection from Signature Mismatch	2,657	1,516
Signature Mismatch Rejection Rate	0.131%	0.079%

Table 2: Comparison of Signature Mismatch Rejection Rates in the **State of Arizona** for 2016 general election with 2018 midterm election.

Table 2 shows that *as the number* of Mail-In ballots in the State of Arizona ***decreased*** from 2,017,722 in the 2016 general election by 118,482 Mail-In ballots to 1,899,240 in the 2018 midterm election, representing a 5.62% ***decrease***, the rejections from Signature Mismatch also ***decreased*** by 1,141 Mail-In ballots, a 42.9% ***decrease*** from 2016 to 2018. In addition, the Signature Mismatch Rejection Rate ***decreased*** from 0.131% in 2016, by 39.7%, to 0.079% in 2018. In summary, ***decreases*** in Mail-In ballots were followed by ***decreases*** in

rejections from Signature Mismatch. This appears to be consistent i.e. less Mail-In ballots, less rejections from Signature Mismatch.

MARICOPA EVB RESULTS SUMMARY

The *November General Election CANVASS* report filed by Maricopa County election officials, documents the various counts for EVB return envelopes, during the 2016 and 2020 general elections. These counts are shown in Figure 7.[20]

MARICOPA COUNTY

VOTER EDUCATION REPORT

2020 PRIMARY & GENERAL ELECTION

GENERAL ELECTION

VOTER TURNOUT	2020	2016
Voter Turnout	80.51%	74.43%
Early Ballots Requested	2,160,412	1,497,565
Early Ballots Verified and Counted	1,915,487	1,251,978
Rejected Early Ballots		
Bad Signatures	587	1,456
No Signatures	1,455	2,209
Late Returns	934	1,536

Figure 7: EVB return envelope metrics for **Maricopa County,** including Verified and Counted, Bad Signatures, No Signatures and Late Returns, as reported in the *CANVASS* report.

Per the report for **Maricopa County** as shown in Figure 7, for 2020, 1,915,487 EVB return envelopes were Verified and Counted (after Signature Verification); 587 were classified as "Bad Signatures;" 1,455 were classified as "No Signatures;" and, 934 were classified as "Late Returns." Summing up these counts yields a total of 1,918,463 unique EVB return envelopes that were processed by Maricopa County election officials in 2020. Similarly,

[20]Voter Education Report, https://recorder maricopa.gov/pdf/11-03-2020-0%20Canvass%20BOS%20SUMMARY%20NOV2020-two-sided%20print.pdf, accessed September 15, 2021

for 2016, 1,251,978 EVB return envelopes were Verified and Counted; 1,456 were classified as "Bad Signatures;" 2,209 were classified as "No Signatures;" and, 1,536 were classified as "Late Returns." Summing up these counts yields a total of 1,257,179 unique EVB return envelopes that were processed by the Maricopa County election officials in 2016. Figure 8 summarizes these results.

Summary of Results from Maricopa County

	Maricopa Reported in 2020	Maricopa Reported in 2016
Unique EVB Return Envelopes	1,918,463	1,257,179
Duplicate Analysis		
Duplicates	NA	NA
Total Unique EVB Return Envelopes	1,918,463	1,257,179
Signature Presence Detection		
No Signature Ballots	(1,455)	(2,209)
Total Ready for Signature Verification	**1,917,008**	**1,254,970**
Signature Verification Process		
"Bad Signatures"	(587)	(1,456)
"Late Returns"	(934)	(1,536)
Total EVBs Verified and Counted	**1,915,487**	**1,251,978**

Figure 8: Results for **Maricopa County**, for 2016 and 2020 general elections, with calculated total of unique EVB return envelopes processed.

Using the data from Figure 8, a comparison chart in Table 3 is created to compare Signature Mismatch Rejection Rates for **Maricopa County** for the 2016 and 2020 general elections. In 2016, the number of unique EVB return envelopes processed is 1,257,179. There are 1,456 EVB return envelopes rejected for "Bad Signatures" i.e. Signature Mismatches. The Signature Mismatch Rejection Rate for **Maricopa County in 2016** is

therefore 0.116%. In 2020, the number of unique EVB return envelopes processed is 1,918,463. There were 587 EVB return envelopes rejected for "Bad Signatures" i.e. Signature Mismatches. The Signature Mismatch Rejection Rate for **Maricopa County in 2020** is 0.031%. These results are consolidated in Table 3.

	Maricopa County, AZ 2020 General Election	Maricopa County 2016 General Election
EVB Return Envelopes	1,918,463	1,257,179
Rejection from Signature Mismatch	587	1,456
Signature Mismatch Rejection Rate	0.031%	0.116%

Table 3: Comparison of Signature Mismatch Rejection Rates in **Maricopa County 2016** general election with **Maricopa County 2020** general election.

Table 3 reveals that *as the number* of EVB return envelopes in Maricopa County ***increased*** from 1,257,179 in the 2016 general election by 661,284 to 1,918,463 unique EVB return envelopes in the 2020 general election, representing a 52.6% ***increase***, the rejections from Signature Mismatches, however, ***decreased*** by 869 EVB return envelopes, a 59.7% ***decrease*** during the same period. In addition, the Signature Mismatch Rejection Rate ***decreased*** from 0.116% in 2016 by 73.3% to 0.031% in 2020. In summary, ***increases*** in EVB return envelopes from 2016 to 2020 were followed by ***decreases*** in Signature Mismatches. This appears to be *inverse* i.e. more EVB return envelopes, ***less*** Signature Mismatches. Maricopa election officials can best answer this inverse relationship.

SCOPE OF AUDIT

Arizona State Senate commissioned EchoMail to perform audit of Signature Presence Detection ***solely within the Signature Region of EVB return envelope images.*** On August 27, 2021, a Master Agreement and Statement of Work ("SOW") were executed by Dr. Shiva Ayyadurai, the President/CEO of EchoMail, Inc., and by Karen Fann, President of the Senate for the Arizona State Senate. Per the SOW, the Arizona State Senate was responsible for:

- Providing the EVB return envelope images that were received by Maricopa County to EchoMail
- Ensuring that the EVB envelope images were delivered to EchoMail via postal mail on a hard drive or uploaded to a secure repository for EchoMail to download

EchoMail was responsible for conducting the following pattern recognition classification processing activities:

- Pre-processing of the EVB return envelope images including auto-aligning, resizing, and calibrating the images to detect the Signature Region
- Detecting the presence of signatures in the Signature Region of the EVB return envelope images
- Detecting if the Signature Region contained a Scribble as recognized by the EchoMail algorithm

- Tabulating a breakdown of the number Signature Regions of the EVB return envelopes with Signatures, with Blanks, and with Scribbles (potentially invalid signatures requiring human review).

On or before September 20, 2021, EchoMail was expected to deliver the following:

- A breakdown of counts of the number of EVB return envelope images where the Signature Region had Signatures, Blanks, and Scribbles
- The images of those EVB return envelopes where the Signature Region was categorized as containing Blanks i.e. "No Signatures"
- The images of those EVB return envelopse where the Signature Region was categorized as containing Scribbles

As of the writing of this report, both parties have met their responsibilities on or before the deadlines established. EchoMail's scope of work, to be clear, was ***not*** to perform Signature Verification, that is to compare the signatures identified in the Signature Region of the EVB return envelope images with signatures stored in an official repository such as voter registration files. EchoMail's role was limited to identifying the presence of a signature in the Signature Region of the EVB return envelope images. ***If a signature appeared elsewhere on the EVB return envelope image, EchoMail was not responsible for detecting or classifying such instances.***

METHODOLOGY

Pattern recognition classification methods are at the core of the methodology for Signature Presence Detection. Pattern recognition classification involves a systematic process of feature detection, clustering, and learning to distinguish "normal" states from "abnormal" states as illustrated in Figure 9.

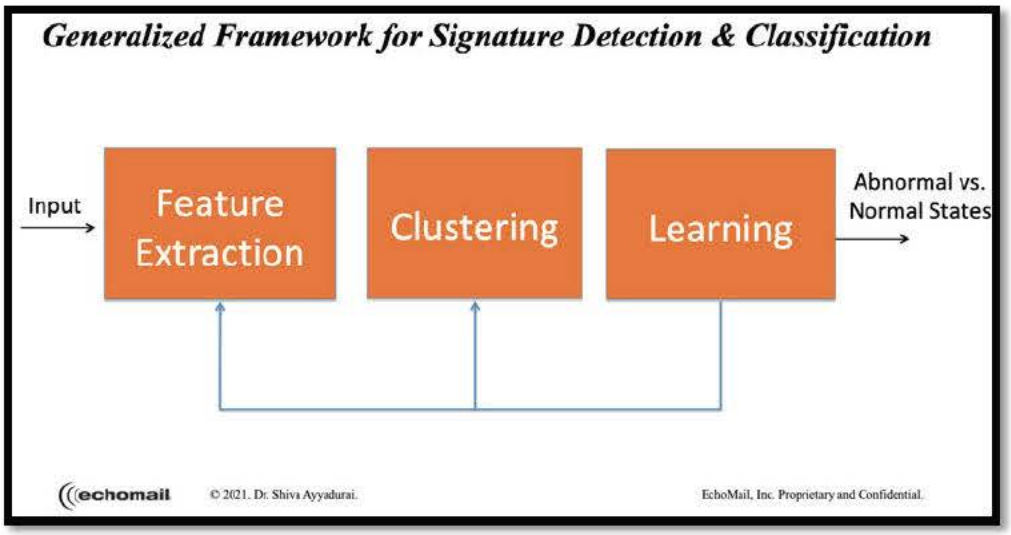


Figure 9: Generalized framework for signature detection and classification.

Given the likely diversity of backgrounds in the readers of this manuscript, fundamental concepts concerning pattern recognition along with a review of this author's – Dr. Shiva's – expertise, across a range of signals and signatures, are provided for the reader to gain a foundational understanding of the field along with an appreciation of the many diverse applications afforded by pattern recognition classification methods.

FOUNDATIONS OF PATTERN RECOGNITION

Consider a basic system with an input and an output as shown in Figure 10. At any point in time, the system possesses a system *state.*

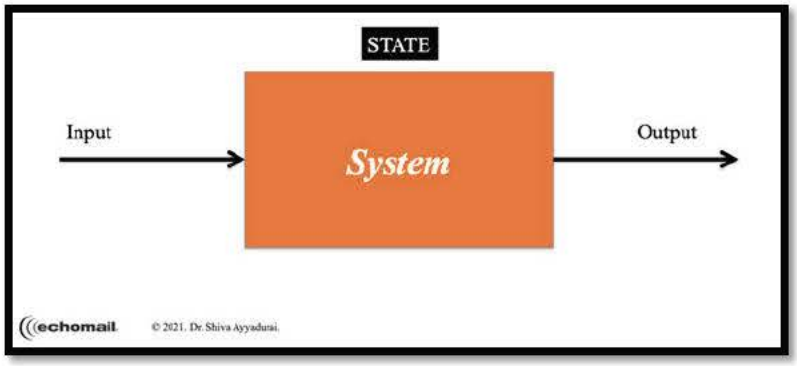


Figure 10: Basic system with input, output, and state.

One aim of pattern recognition classification methods is to identify system states, which may be the system's desired or "Normal State" as denoted in Figure 11, determined by the system's input and output behavior.

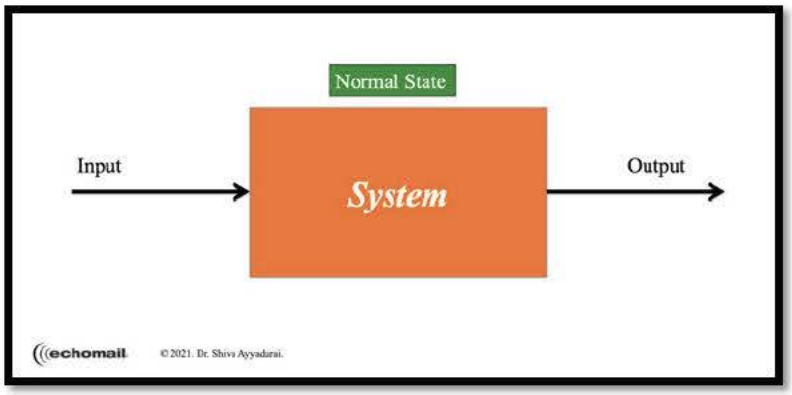


Figure 11: A system in a "Normal State" as a function of its input-output behavior.

Or, pattern recognition classification methods are applied to determine the anomalous states or "Abnormal State" of a system as denoted below on Figure 12.

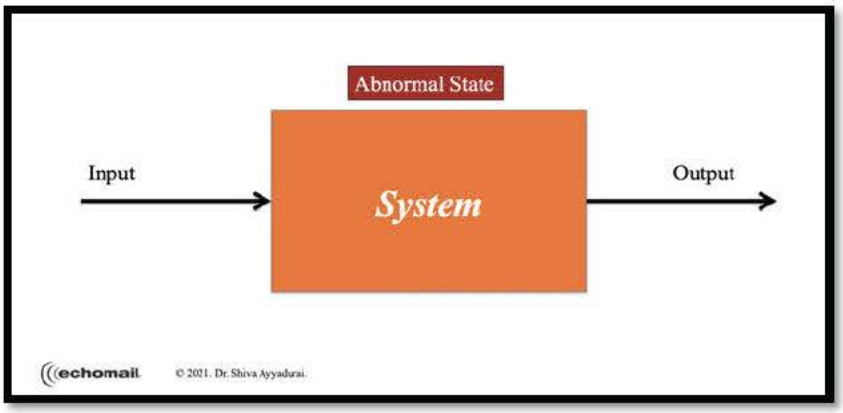


Figure 12: A system in an "Abnormal State" as a function of its input-output behavior.

Feature extraction approaches are used to develop a signature/signal to identify the states of a system, be they the Normal State or the Abnormal State. For example, in Figure 13, a signal representing the Normal State of a cardiovascular system is illustrated.

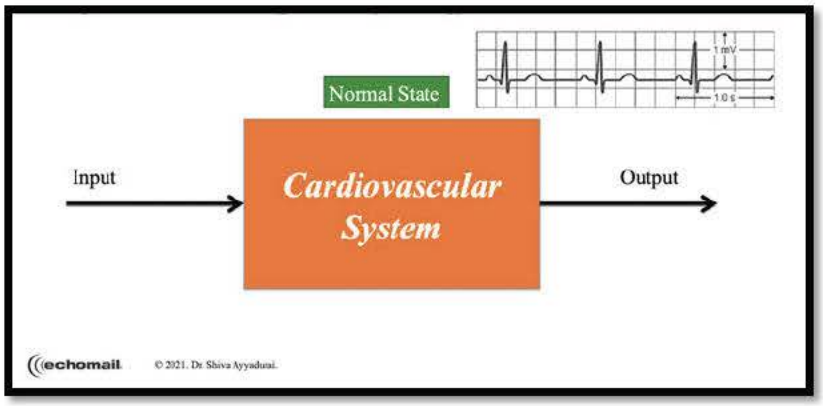


Figure 13: The cardiovascular system in its Normal State.

In Figure 14, a signature/signal of the cardiovascular system reflecting its Abnormal State is illustrated; in this case, the system's signature represents the heart in distress e.g.

ventricular fibrillation.

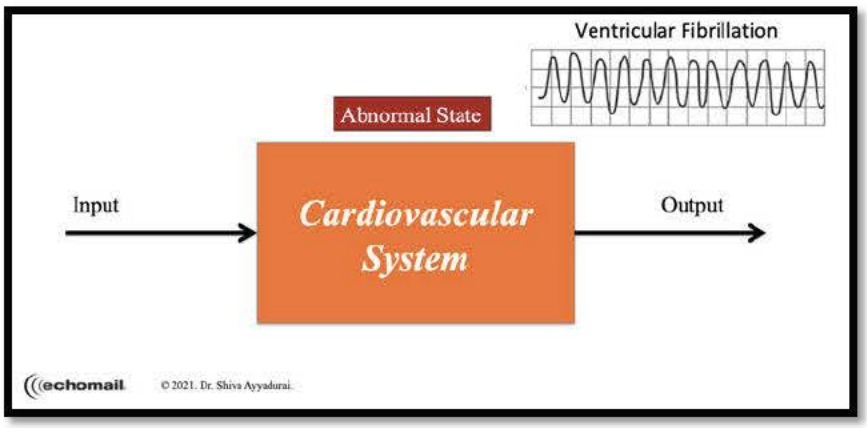


Figure 14: The cardiovascular system in an Abnormal State: ventricular fibrillation.

Figure 15 illustrates for a cardiovascular system, signature for the Normal State and several signatures for the Abnormal State.

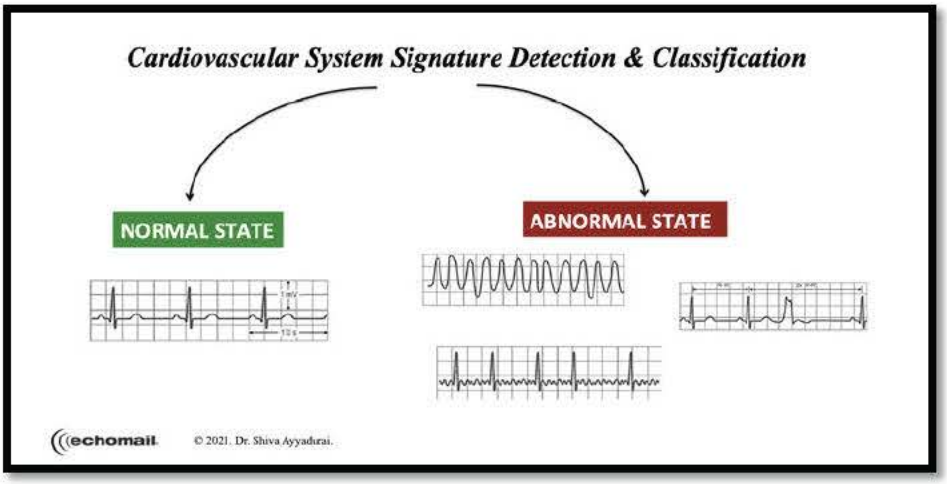


Figure 15: Pattern recognition classification of cardiac signatures in Normal and Abnormal States.

For the audit herein, the same approach is employed to define the Normal State as a Signature Region with a Signature, and the Abnormal States as those Signature Regions

with Blank, Likely Blank, and Scribble, as illustrated in Figure 16.

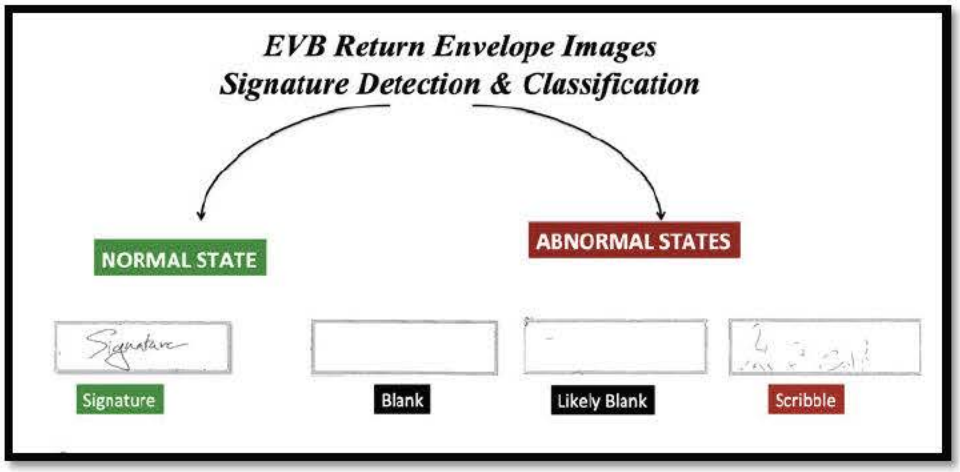


Figure 16: Pattern recognition classification of EVB return envelope images into Normal State with Signature, and Abnormal States: with Blank, Likely Blank and Scribble.

PATTERN RECOGNITION EXAMPLES

Pattern recognition classification methods can be applied to a diversity of problems. Sharing the portfolio of the author's research and development efforts in the field will provide the reader with a glimpse of that diversity, which traverse signals and signatures across a range of industries: biology and medicine, engineering (e.g. aeronautical, civil, mechanical, and electrical), banking, finance, and, government.

Sudden Infant Death Syndrome (SIDS) Research (1978 – 1984)

Sudden Infant Death Syndrome (SIDS) is the leading cause of death in babies between one month and one year of age. In 1978, Dr. Shiva's interest in pattern recognition first began, when as a 14-year-old he was recruited by the University of Medicine and Dentistry of New Jersey (UMDNJ) in Newark, NJ as a Research Fellow.

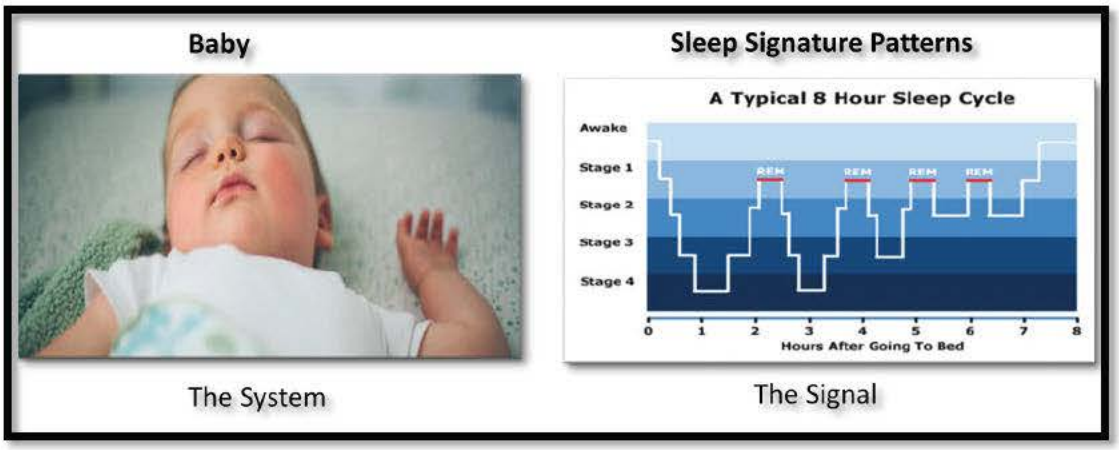


Figure 17: Signature Detection and Classification of Abnormal Sleep Patterns in Babies with Sudden Infant Death Syndrome (SIDS) – (1978 – 1984).

His medical research at UMDNJ focused on developing pattern recognition classification

methods for categorization of sleep signature patterns from babies with SIDS. His research identified certain signatures of waiting times of babies' sleep transition states i.e. the Abnormal States, that appeared to occur before the onset of apneas i.e. when the baby stops breathing. His work led to a scientific paper published and presented at the IEEE/EMBS International Conference in Espoo, Finland.

Tadoma Research (1983 – 1986)

Tadoma is a means of communication used by the deafblind. In this approach, the deafblind person places their right or left hand, and the fingers on the face of a person. The tactile functions of the hand are able to perceive the airflow, vibrations, jaw locations, lip location, and protrusions to sense speech, as illustrated in Figure 18,

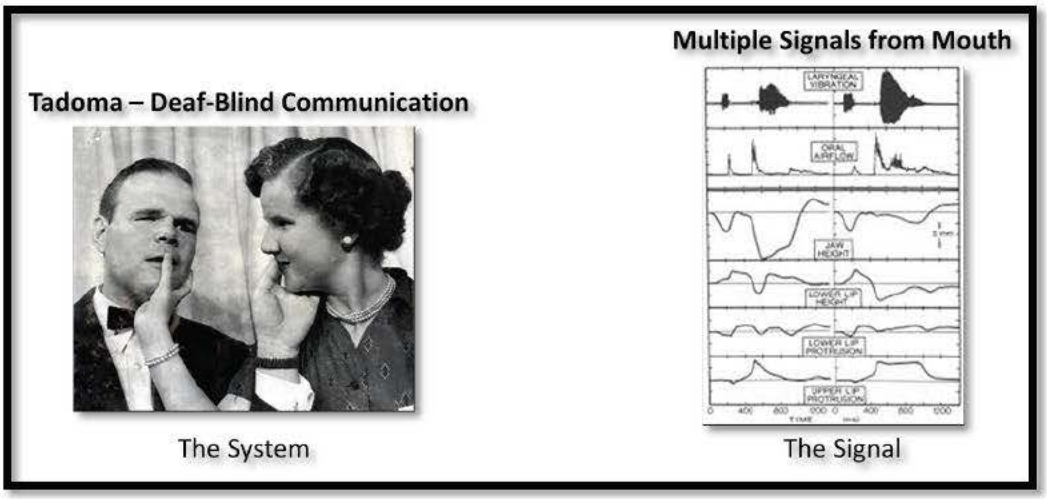


Figure 18: Signal Detection in Tadoma of Non-Vocal Communication for Supporting Deaf-Blind (1983-1986).

During 1983 to 1986, Dr. Shiva's research at the MIT Speech Laboratory, through the MIT Undergraduate Research Opportunities Program (UROP), served to help categorize

specific signatures of these facial movements towards aiding researchers to identify the mechanisms of Tadoma.

Non-Destructive Evaluation (NDE) for Bridge Deck Deterioration (1986 - 1988)

It is estimated that more than 50,000 bridges in the United States are falling apart with varying types of decay and failure. Identifying the nature of these failures, using non-invasive approaches can save time and money. In 1986, under an NSF funded project in the MIT Department of Civil Engineering, Dr. Shiva created algorithms for classification of bridge deck deterioration signatures acquired from radar analysis.

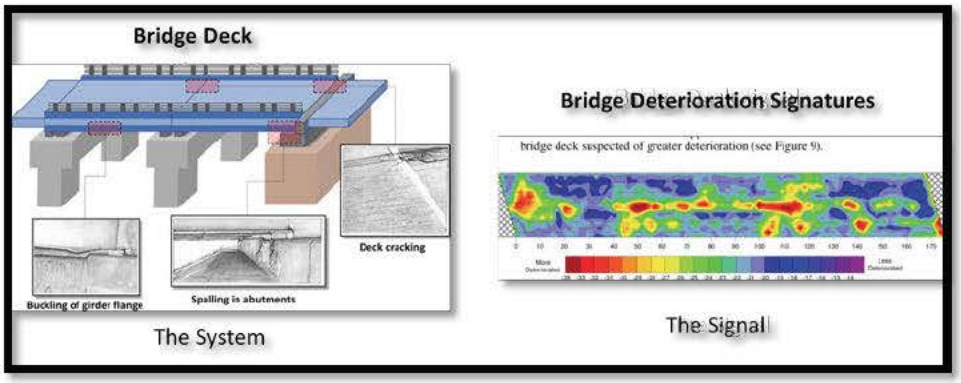


Figure 19: Signal Detection of Flaws in Bridges for Prediction of Bridge Deck Failures (1986-1988).

Such research known as Non-Destructive Evaluation (NDE) aimed to identify flaws in large structures such as bridges, without invasive interventions, to prevent damage and potentially save lives by addressing structural issues before onset of a failure.

Non-Destruction Testing (NDT) of Composite Parts of Aircraft Wings (1988-1990)

Aerospace parts, such as the wings of an aircraft, may consist of flaws and incongruencies that can lead to catastrophic failures.

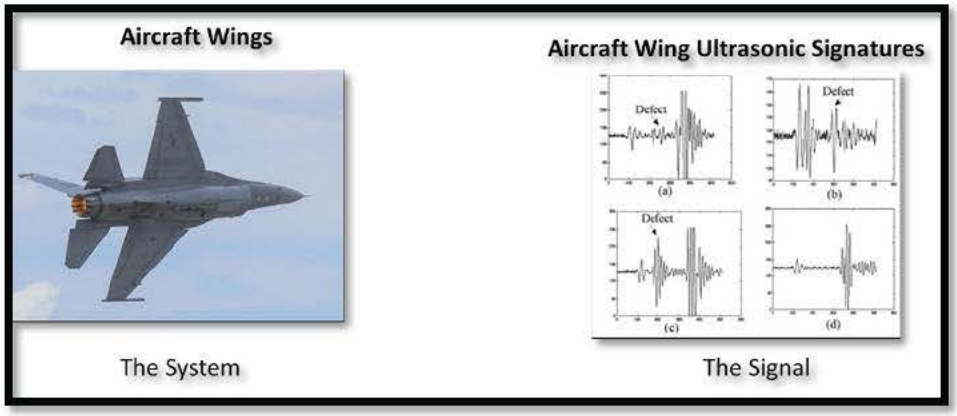


Figure 20: Signal Detection of Ultrasonic Signals for Preventative Maintenance of Composite Aircraft Wings (1988-1990).

In the aerospace industry, non-destructive testing (NDT) is a critical component in efforts to decrease the risk of potentially fatal failures. Dr. Shiva's research in applying pattern recognition for NDE of bridge decks evolved to his Masters work at MIT in the Department of Mechanical Engineering where he developed a computational model of wave propagation in composite materials, that he used to create unsupervised pattern recognition classification methods for NDT of composites in order to characterize flaws and irregularities in objects such as aircraft wings. The research aimed to classify signals in order to support preventative maintenance of structures like aircraft wings without disrupting their integrity.

Handwritten Numerals on Bank Checks (1992-1994)

Even though online banking has grown, there still continues to be a need for processing paper checks.

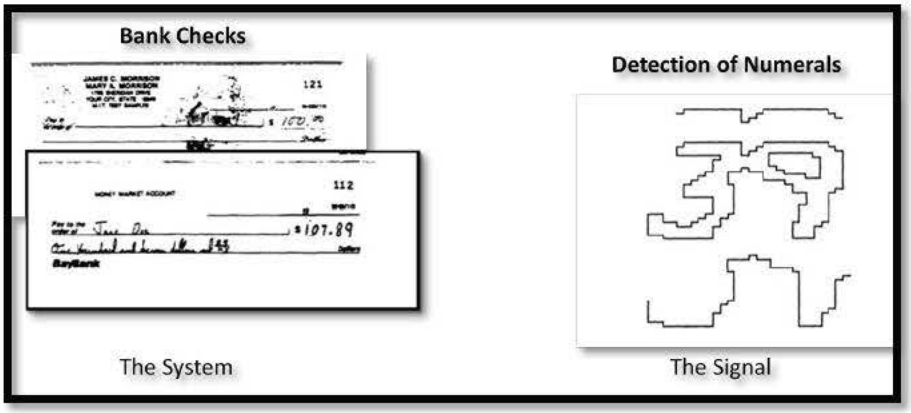


Figure 21: Integrated Architecture for Recognition of Handwritten Numerals on Bank Checks (1992-1994).

For his PhD work, starting in 1990, Dr. Shiva set out to create a generalized framework, which he termed *Information Cybernetics*, for solving diverse pattern recognition problems. In 1992, he began work with researchers at the MIT Sloan School on a project to automatically recognize the courtesy amount on bank checks. This effort resulted in his leading an MIT team to architect and create a fully working prototype of a hybrid neural network based system for pattern recognition of the courtesy amount on bank checks, which he successfully demonstrated to NatWest Bank. The work resulted in a pioneering paper in the *International Journal of Pattern Recognition and Artificial Intelligence (IJPRAI)* in 1993.

EchoMail®: Automatic Document Analysis and Classification (1993-Present)

Following the invention of email by Dr. Shiva in 1978, and up until 1993, email was an inter- and intra- office business application. However, after the advent of the World Wide Web (WWW) in 1992, web-based email applications made email a consumer application resulting in an explosive growth of email usage.

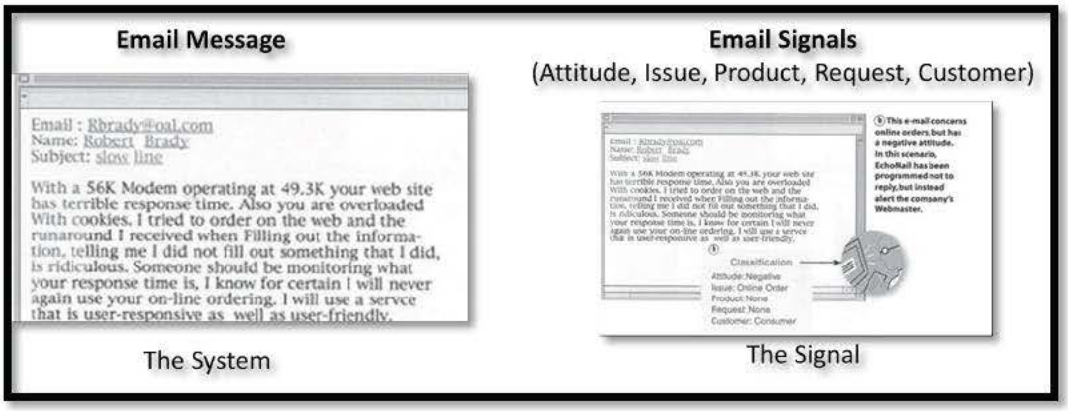
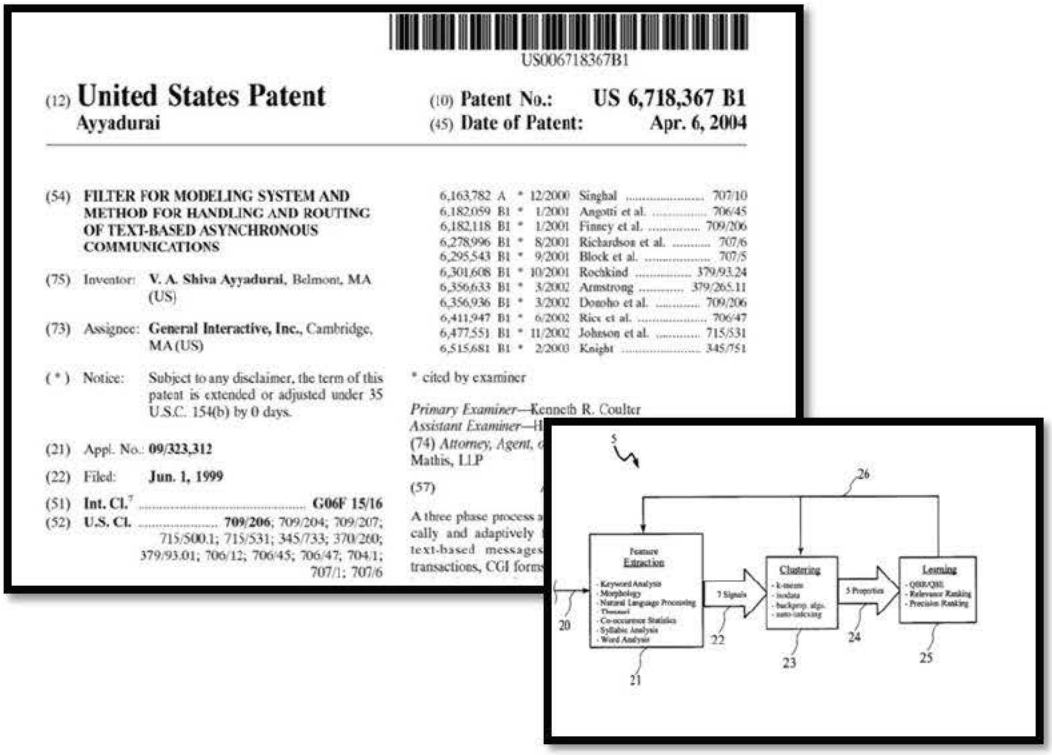


Figure 22: Signal Detection of Email Signals for Automatic Categorization (1992 - Present).

In 1993, the White House, Executive Office of the President, sponsored an industry-wide competition to automatically to analyze and classify President Clinton's email to assist in handling the deluge of email. While in the midst of his PhD work, after being selected as the only student participant, Dr. Shiva won this industry-wide competition. This resulted in his being awarded a number of foundational patents in pattern recognition (one of which is shown in Figure 23) and developing EchoMail® - a platform for enabling pattern recognition classification of electronic documents, which led to his starting EchoMail, Inc., a company that grew to nearly $200 million in market valuation. EchoMail was featured in

a front-page article in *The MIT Technology Review*, the leading magazine for technology.[21]

EchoMail enabled the automatic classification and routing of large volumes of email for Global 2000 companies such as Nike, American Express, P&G, Citigroup, to enable rapid response to customer inquiries, as well as to increase levels of customer service.


US006718367B1

(12) **United States Patent**
Ayyadurai

(10) **Patent No.: US 6,718,367 B1**
(45) **Date of Patent: Apr. 6, 2004**

(54) **FILTER FOR MODELING SYSTEM AND METHOD FOR HANDLING AND ROUTING OF TEXT-BASED ASYNCHRONOUS COMMUNICATIONS**

(75) Inventor: **V. A. Shiva Ayyadurai**, Belmont, MA (US)

(73) Assignee: **General Interactive, Inc.**, Cambridge, MA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/323,312**

(22) Filed: **Jun. 1, 1999**

(51) **Int. Cl.**[7] **G06F 15/16**

(52) **U.S. Cl.** **709/206**; 709/204; 709/207; 715/500.1; 715/531; 345/733; 370/260; 379/93.01; 706/12; 706/45; 706/47; 704/1; 707/1; 707/6

6,163,782	A *	12/2000	Singhal	707/10
6,182,059	B1 *	1/2001	Angotti et al.	706/45
6,182,118	B1 *	1/2001	Finney et al.	709/206
6,278,996	B1 *	8/2001	Richardson et al.	707/6
6,295,543	B1 *	9/2001	Block et al.	707/5
6,301,608	B1 *	10/2001	Rochkind	379/93.24
6,356,633	B1 *	3/2002	Armstrong	379/265.11
6,356,936	B1 *	3/2002	Donoho et al.	709/206
6,411,947	B1 *	6/2002	Rice et al.	706/47
6,477,551	B1 *	11/2002	Johnson et al.	715/531
6,515,681	B1 *	2/2003	Knight	345/751

* cited by examiner

Primary Examiner—Kenneth R. Coulter
Assistant Examiner—H
(74) *Attorney, Agent,*
Mathis, LLP

(57)

A three phase process
cally and adaptively
text-based messages
transactions, CGI forms

Figure 23: One of Dr. Shiva Ayyadurai's U.S. patents for pattern recognition classification.

The approach here, as aforementioned, was to identify the Normal State as well as the Abnormal States of an email, as illustrated in Figure 24.

[21] Dr. Email Will See You Now, MIT Technology Review, https://vashiva.com/wp-content/uploads/2019/12/2000_tech_review.pdf, accessed September 15, 2021

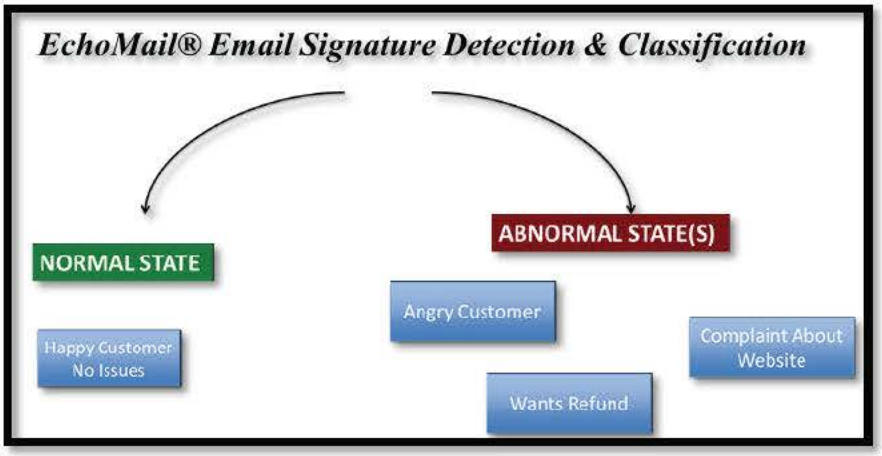


Figure 24: Signal Detection of Email Signals for Automatic Categorization into Normal and Abnormal States.

CytoSolve®: Discovering Combinations That Work (2007-Present)

Modern pharmaceutical companies spend upwards of $5 billion and up to 13 years of research and development to discover and get a single molecule drug to market. However, the future of medicine demands the need for multi-combination therapies i.e. "cocktails," which are not possible with conventional approaches. Such efforts require a computational systems biology approach integrating pattern recognition methods.

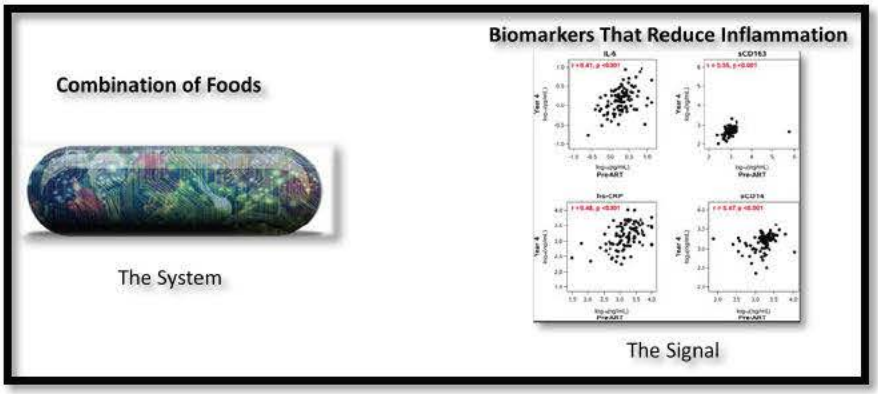


Figure 25: Signal Detection of Combination Therapies that Alleviate Disease (2007 - Present).

In 2003, Dr. Shiva returned to MIT to complete his doctoral work in computational systems biology in the department of Biological Engineering, where he developed CytoSolve®, a scalable computational systems biology platform for modeling the whole cell by dynamic integration of molecular pathways models. CytoSolve computationally models complex diseases and biomolecular processes to discover multi-combination therapeutics by identifying biomarker signatures that are associated with optimal combinations. CytoSolve earned an FDA allowance in a record 11 months for a multi-combination therapy for pancreatic cancer. Today, CytoSolve is being used to develop a diverse range of innovative multi-combination products from natural sources, across a variety of indications including pain, inflammation, oral health, brain health, and relaxation, to name a few.

As should be evident, from these examples, pattern recognition classification methods can be applied to a range of problems.

MATHEMATICAL MODELING

Pattern recognition is reliant on two aspects: mathematical modeling and signature/signal detection and classification. Mathematical modeling, as illustrated in Figure 26, involves observing a system, making hypothesis, manipulating the system, measuring input and output behavior, from which data is mined, to create mathematical models to understand why and how the system operates.

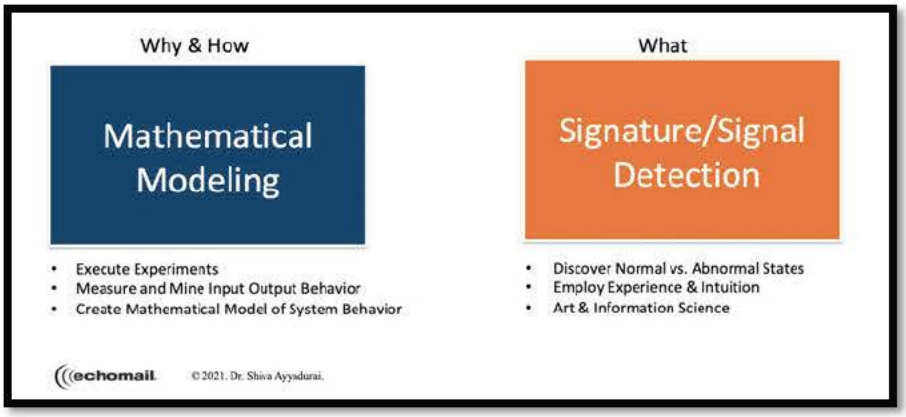


Figure 26: The two aspects of pattern recognition.

Here, the scientific method is employed, as best exemplified in Newton's observation of a pattern of behavior in the natural world between two masses, to elicit a mathematical model, known as Newton's Law of Universal Gravitation, as illustrated in Figure 27.

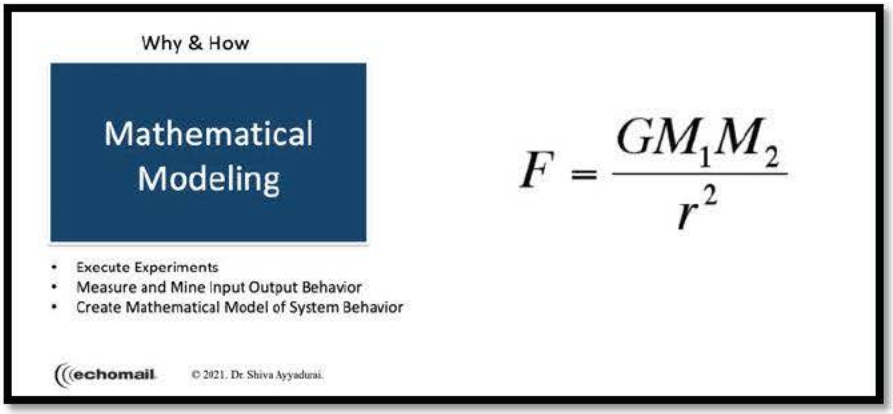


Figure 27: Newton's application of pattern recognition and use of mathematical modeling let to Newton's Law of Universal Gravitation.

Mathematical modeling provides the ability to simulate potential input and output behavior as a vehicle to understand potential states of a system. Such models can provide insights into likelihood of normal or anomalous behavior.

SIGNATURE/SIGNAL DETECTION & CLASSIFICATION

Signature or (signal) detection and classification methods, the other aspect of pattern recognition, aims to document and characterize the signatures or signals of a system, some which may reflect normal, and others, abnormal behavior. Signature detection, unlike mathematical modeling, is derived from domain and subject matter expertise using intuition, and an integration of art and information science, as shown in the right hand side of Figure 26. The reductionist application of mathematical techniques, simple or sophisticated, without knowledge of the domain can lead to significant and serious errors. Mathematics is not a sufficient knowledge base to solve real life problems in the domain of pattern recognition.

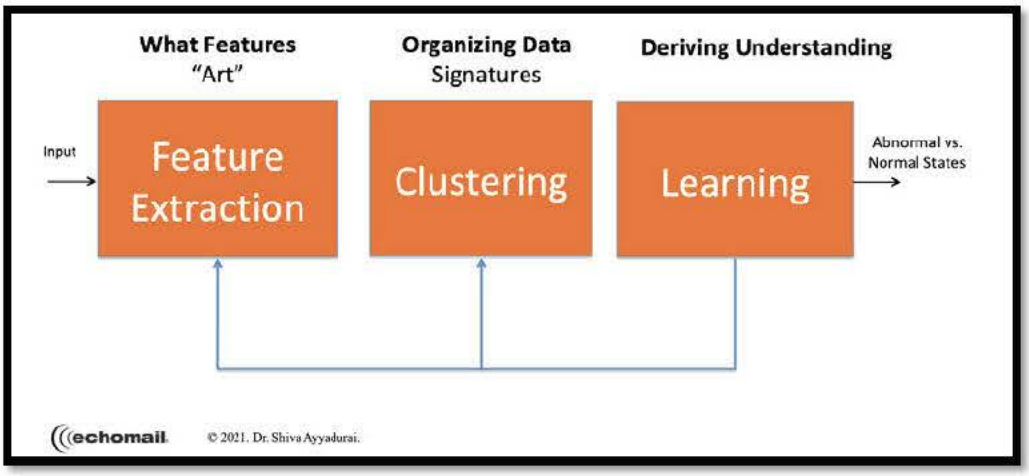


Figure 28: Signature/signal detection and classification are both an art and an information science relying on feature extraction, clustering and learning.

In this aspect, feature extraction – the art of pattern recognition –, as illustrated in Figure 28, becomes critical to deriving features that can best be used to describe the signature or signal of the system. For example, in the field of face detection, prior to this foundational

understanding, researchers focused on two-dimensional image processing methods, brute force computations methods to capture and process as much image pixel information as possible, believing more resolution the better. However, pattern recognition reveals the need to focus on the art of identifying key features, as shown in Figure 30, where a handful of numbers could capture critical features for classification, such as the overall shape of the face e.g. square, oval, rectangular; distance measurements between the eyes, nose and mouth; or, combinations thereof, that could be sufficient to derive a reasonable identification of a face using other contextual data.

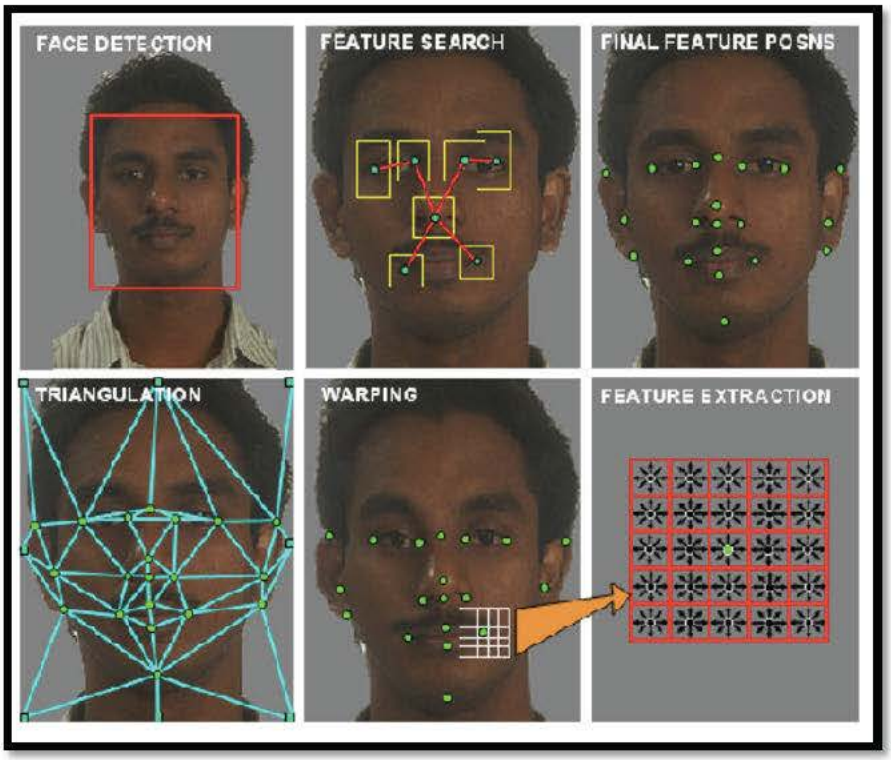


Figure 30: Feature extraction process to enable face detection. [22]

[22] Prince, Simon & Elder, James & Hou, Yunhe & Sizinstev, M. & Olevsky, E.. (2006). Towards Face Recognition at a Distance. 570 - 575. 10.1049/ic:20060363.

EVB RETURN ENVELOPE IMAGE CLASSIFICATION

Pattern recognition classification methods are employed in this audit by EchoMail using the aforementioned foundational processes to identify the specific Signature Region of EVB return envelope images. and classify it into one of four specific categories: Signature, Blank, Likely Blank, and Scribble as illustrated in Figure 31.

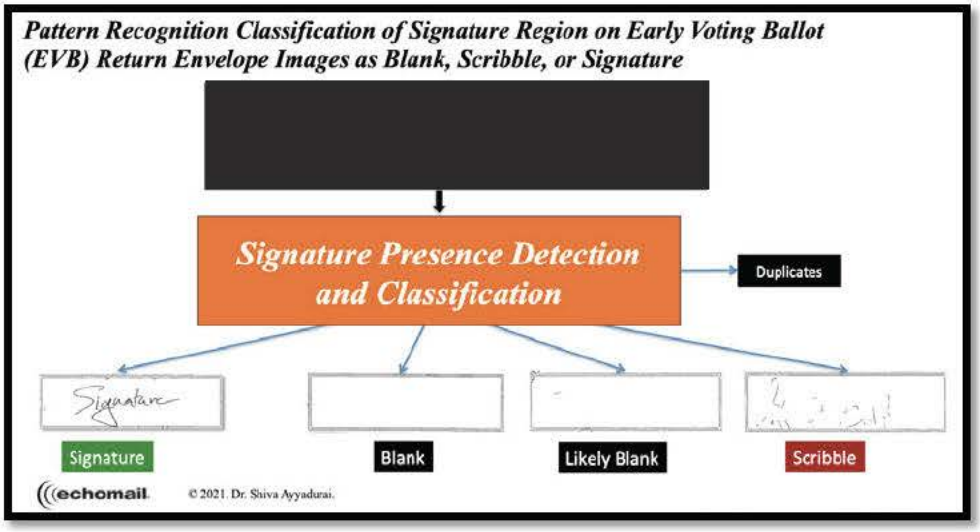


Figure 31: Pattern recognition classification of Signature Region of EVB return envelope images into Signature, Definitive Blank, Likely Blank, and Scribble.

The first step in this classification process is the acquisition and data warehousing of the data set of EVB return envelope image files, as discussed below in *Date Set of EVB Return Envelope Images*. The second step is the execution of the EchoMail Signature Presence Detection System (SPDS) to: 1) identify Duplicates among EVB return envelope images; 2) identify the Signature Region; and, 3) classify the Signature Region into Signature, Blank, Likely Blank or Scribble. This process is discussed below in *EchoMail EVB Signature Presence Detection System.*

DATA SET OF EVB RETURN ENVELOPE IMAGES

The data set containing the EVB return envelope image files was delivered to EchoMail from the Arizona State Senate on a hard drive. The hard drive contained the following two main directories as shown in Figure 30.

Name	Date modified	Type
Alternate Return - Format Early Affidavits	8/17/2021 6:41 PM	File folder
EarlyVotingSignatures	8/2/2021 1:53 PM	File folder

Figure 32: Two main directories on hard drive received from the Arizona State Senate.

The "EarlyVotingSignatures" directory contained 182 sub-folders, as shown in Figure 31.

Name	Date modified	Type
PBSigVar_1377_RTNIMAGOUT_10092020_0001	8/2/2021 5:07 PM	File folder
PBSigVar_1377_RTNIMAGOUT_10102020_0002	8/2/2021 7:41 PM	File folder
PBSigVar_1377_RTNIMAGOUT_10102020_0003	8/3/2021 2:55 AM	File folder
PBSigVar_1377_RTNIMAGOUT_10122020_0004	8/2/2021 7:38 PM	File folder
PBSigVar_1377_RTNIMAGOUT_10122020_0005	8/3/2021 12:21 AM	File folder
PBSigVar_1377_RTNIMAGOUT_10122020_0006	8/3/2021 6:08 AM	File folder
PBSigVar_1377_RTNIMAGOUT_10122020_0007	8/3/2021 9:48 AM	File folder
PBSigVar_1377_RTNIMAGOUT_10132020_0008	8/2/2021 2:31 PM	File folder
PBSigVar_1377_RTNIMAGOUT_10132020_0009	8/2/2021 6:07 PM	File folder
PBSigVar_1377_RTNIMAGOUT_10142020_0010	8/2/2021 10:41 PM	File folder
PBSigVar_1377_RTNIMAGOUT_10142020_0011	8/2/2021 8:15 PM	File folder
PBSigVar_1377_RTNIMAGOUT_10142020_0012	8/3/2021 1:39 AM	File folder
PBSigVar_1377_RTNIMAGOUT_10142020_0013	8/3/2021 6:39 AM	File folder
PBSigVar_1377_RTNIMAGOUT_10142020_0014	8/3/2021 10:15 AM	File folder
PBSigVar_1377_RTNIMAGOUT_10142020_0015	8/3/2021 11:45 AM	File folder

Figure 33: Structure of the EarlyVotingSignatures main directory and example of its sub-folders. There are 182 sub-folders, in total.

Each sub-folder contained the vast majority of the EVB return envelope files, which are denoted as standard image files (SIF), in TIFF format and look as shown in Figure 34.

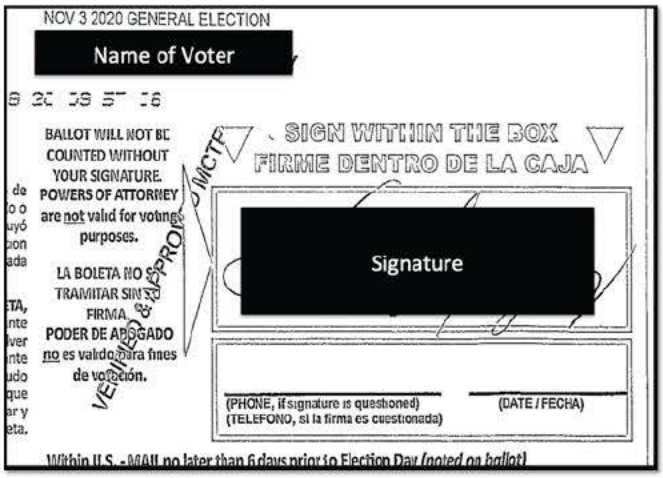


Figure 34: Standard Image Files in TIFF format.

The second main directory named "Alternate Return – Format Early Affidavits" contained six PDF files as shown in Figure 35.

Name	Date modified	Type	Size
1 - UOCAVA - SEB Early Ballot Affidavits Box 1	8/17/2021 4:51 PM	Microsoft Edge P...	343,250 KB
2 - UOCAVA - SEB Early Ballot Affidavits Box 2	8/17/2021 4:53 PM	Microsoft Edge P...	292,112 KB
3 - UOCAVA - SEB Early Ballot Affidavits Box 3	8/17/2021 4:56 PM	Microsoft Edge P...	389,393 KB
4 - UOCAVA - SEB Early Ballot Affidavits Box 4	8/17/2021 5:48 PM	Microsoft Edge P...	390,773 KB
5 - Large Print Affidavits Box 5	8/17/2021 5:55 PM	Microsoft Edge P...	50,877 KB
6 - Braille Affidavits Box 6	8/17/2021 5:57 PM	Microsoft Edge P...	369 KB

Figure 35: "Alternate Return – Format Early Affidavits" directory.

The first four PDF files are the UOCAVA image files (UIF) containing three types of image files denoted as UIF-A, UIF-B, and UIF-C, shown in Figures 36-38, respectively.

Figure 36: UOCAVA Image File, Type A (UIF-A).

Figure 37: UOCAVA Image File, Type B (UIF-B).

Figure 38: UOCAVA Image File, Type C (UIF-C).

The fifth PDF file, Large Print Affidavits contains Large Image Files, denoted as "LIF," and is shown in Figure 39. The sixth PDF file, Braille Affidavits contains Braille Image Files, denoted as "BIF," and is shown in Figure 40.

Figure 39: Large Print Image File, (LIF).

Figure 40: Braille Image File, (BIF).

All of the above image formats were extracted from the directories, subfolders, and files into EchoMail's relational database. Once this process was complete, the EchoMail EVB Signature Presence Detection System (SPDS) is deployed. The rapid deployment of this system for this audit was made possible given the rich history of Dr. Shiva's expertise and EchoMail's capabilities.

ECHOMAIL EVB SIGNATURE PRESENCE DETECTION SYSTEM

The pattern recognition infrastructure at EchoMail was used to deploy the EchoMail EVB Signature Presence Detection System (SPDS) as illustrated in Figure 41. The system consists of multiple processes. The first process is the automatic classification and detection of the EVB return envelope type, among the six image formats.

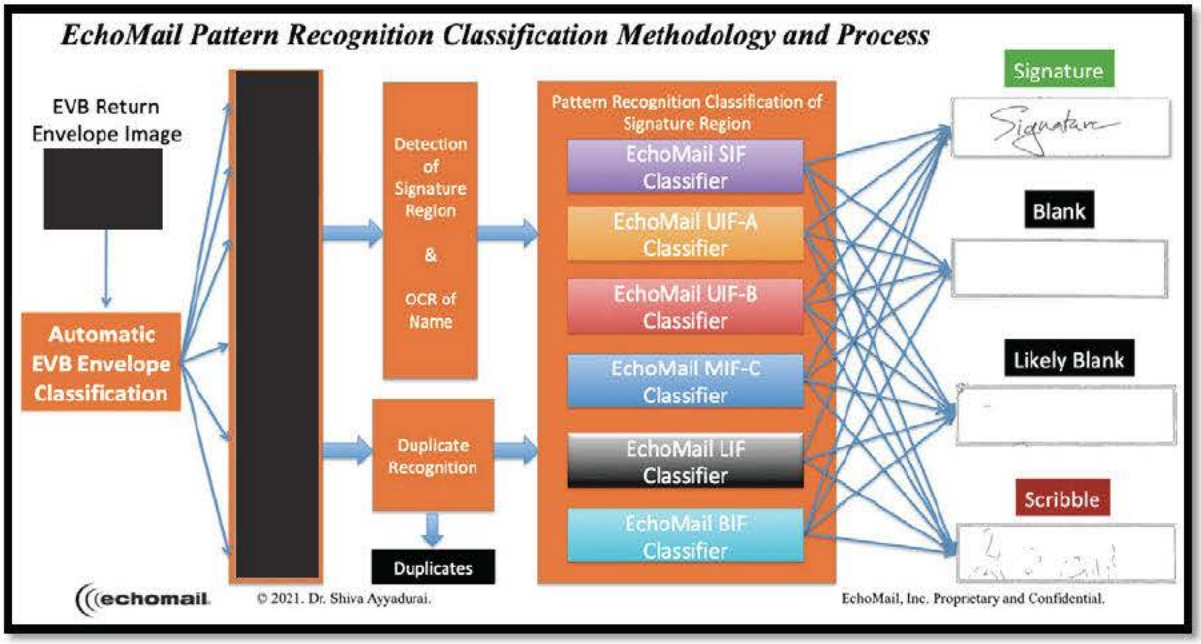


Figure 41: EchoMail EVB Signature Presence Detection System.

As aforementioned, there are six potential image formats. Once this classification – Automatic EVB Envelope Classification – is complete, then the system performs Duplicate Recognition to detect Duplicate EVB return envelope images. Duplicates are properly

classified and tagged. Following this, the system performs a variety of feature extraction methods to detect the Signature Region. For each of the six image types, there are different EchoMail Classifiers as shown in Figure 41 for classifying the different morphologies of Signature Regions.

If the Signature Region has a non-white pixel density of 0%, the EVB return envelope image is classified as a Blank; if the Signature Region has a non-white pixel density of 0%+ to 0.1%, the EVB return envelope image is classified as a Likely Blank; if the Signature Region has a non-white pixel density of 0.1%+ to 1%, the EVB return envelope image is classified as a Scribble; and, finally, if the Signature Region has a non-white pixel density of greater than 1%, the EVB return envelope image is classified as a Signature.

It is important to note that some voters submitted EVB return envelopes with their signature in other areas e.g. in the phone area; however, per the Scope of Audit, only the Signature Region was used for analysis. The EchoMail Analysis offered a relatively low non-white pixel density threshold e.g. 1%+ for Signature Region to be classified as having a Signature.

Though not within the *Scope of Audit*, if possible, EchoMail attempted to find the region with the name of the voter, and performed OCR to capture and store the name in the database.

Once the images are classified, Duplicates are further classified as shown in Figure 42.

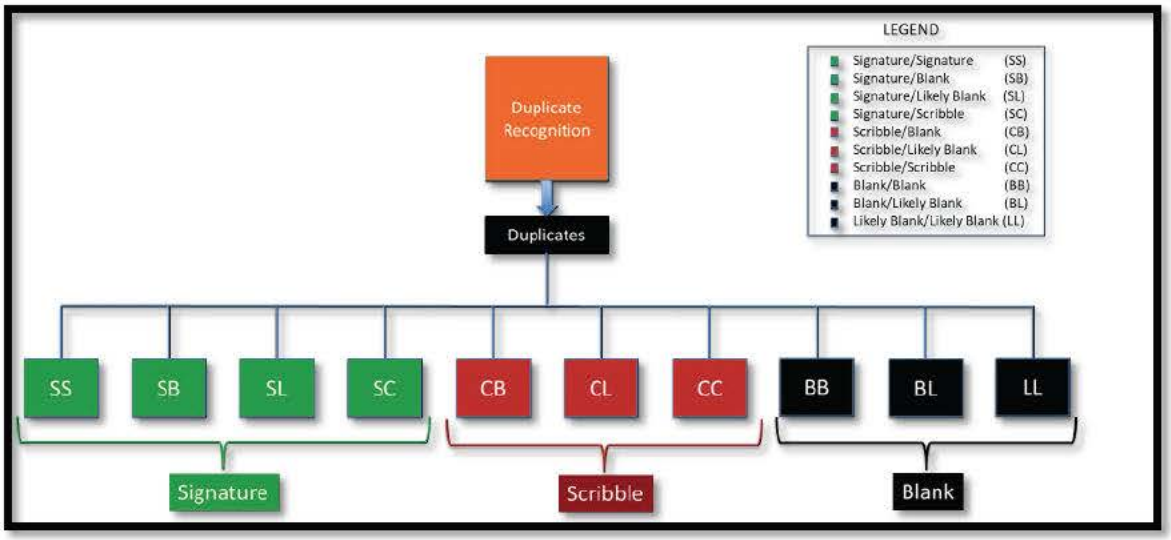


Figure 42: Duplicate Classification of 2-Copy Duplicates.

RESULTS

There are multiple sets of results, that are directly an outcome of a particular process executed from the EchoMail EVB Signature Presence Detection System

EVB RETURN ENVELOPE IMAGES COUNT

A total of 1,929,240 EVB return envelope images were received by EchoMail as summarized in Table 4.

Type of Image	Count	Percent
SIF	1,919,598	99.5%
UIF-A	8,849	0.459%
UIF-B	277	0.014%
UIF-C	12	0.001%
LIF	475	0.024%
BIF	29	0.002%
TOTAL	**1,929,240**	**100%**

Table 4: Total Count of EVB Return Envelope Image Files Received by EchoMail.

There were 1,919,598 SIFs across the 182 sub-folders of the main directory. In the other main directory, there were six files in PDF format containing a total of 9,642 image files. More specifically, there are 9,138 UOCAVA Image Files denoted as "UIF" in the first four PDFs: 8,849 UIF-A type, 277 UIF-B type, and 12 UIF-C type. In the fifth PDF, there are 475 Large Print Affidavits denoted as Large Image Files "LIF." Finally, in the sixth PDF, there are 29 Braille Affidavits (6) denoted as Braille Image Files "BIF."

DUPLICATES ANALYSIS

The results of Duplicate analysis of the EVB return envelope images are summarized in Table 5. As the table reveals 17,126 unique voters submitted a total of 34,448 2-Copy, 3-Copy, and 4-Copy Duplicates.

Type	Total Images	Duplicate Images	Unique # of Voters
2-Copy Duplicates	33,868	16,934	16,934
3-Copy Duplicates	564	376	188
4-Copy Duplicates	16	12	4
Total	34,448	17,322	17,126

Table 5: EchoMail Analysis results of 2-Copy, 3-Copy, and 4-Copy Duplicates. 17,126 unique voters submitted 34,448 Duplicates.

UNIQUE EVB RETURN ENVELOPE IMAGES

Per the results in Table 5, 17,322 Duplicates are removed to produce a count of the total unique EVB return envelope images, which are 1,911,918, as shown in Table 6 below.

	EchoMail Analysis
EVB Return Envelopes Received	1,929,240
Duplicate Analysis	
Duplicates	(17,322)
Total Unique EVB Return Envelopes	**1,911,918**

Table 6: EchoMail Identified 17,322 Duplicates.

DUPLICATE IMAGE EXAMPLES

Below are provided a sampling of the ten (10) different kinds of Duplicates' examples corresponding to the classifications identified earlier in Figure 42. Some of the examples document EVB return envelopes in which, after adjudication, they are stamped with **"VERIFIED & APPROVED MCTEC"**

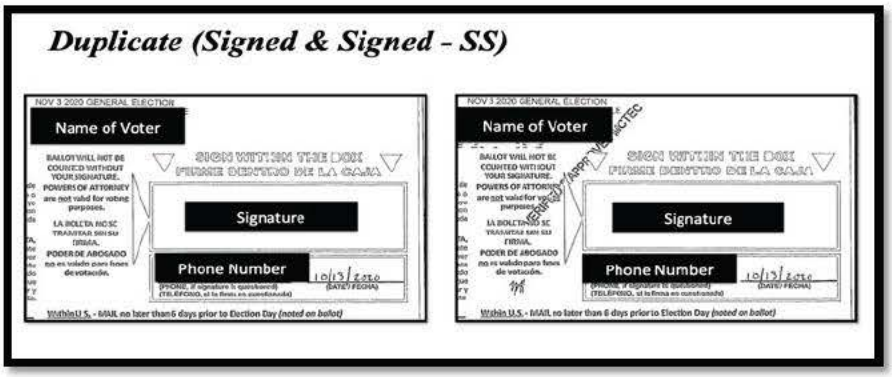


Figure 43: Signed-Signed Duplicate.

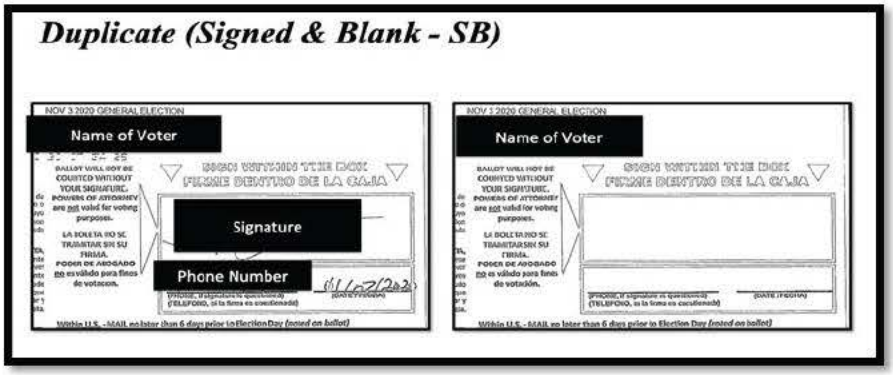


Figure 44: Signed & Blank Duplicate.

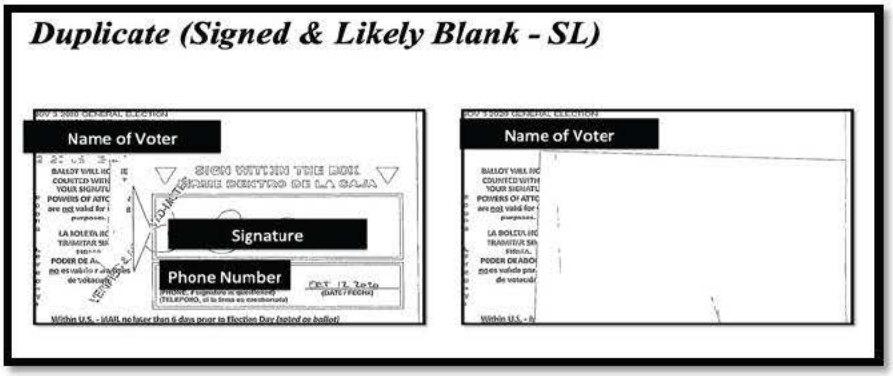


Figure 45: Signed & Likely Blank Duplicate.

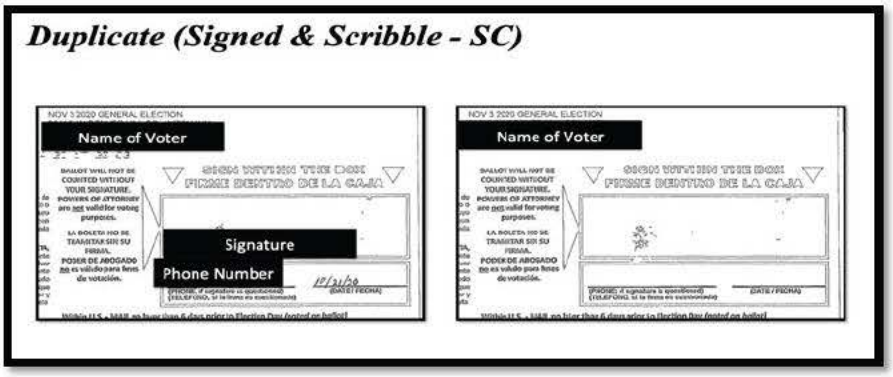


Figure 46: Signed & Scribble Duplicate.

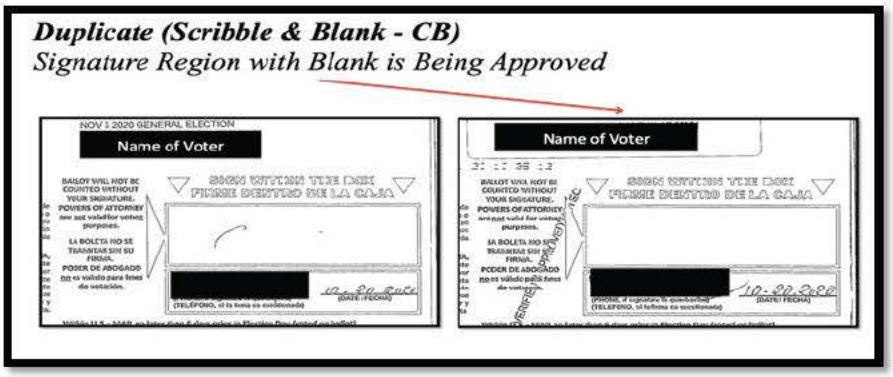


Figure 47: Scribble & Blank Duplicate.[23]

[23] Per the *Scope of Audit*, EchoMail solely analyzes the Signature Region. The Signature Region on the right image, by EchoMail, is classified as Blank regardless of the voter placing their signature elsewhere. During Signature Verification, reviewers may resolve such issues when voters do not follow the explicit instructions, **"SIGN WITHIN THE BOX or FIRME DENTRO DE LA CAJA,"** through a process called adjudication.

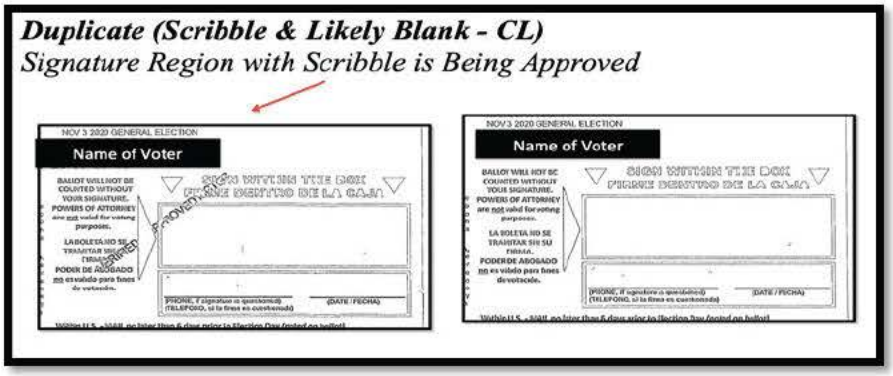


Figure 48: Scribble & Likely Blank Duplicate.

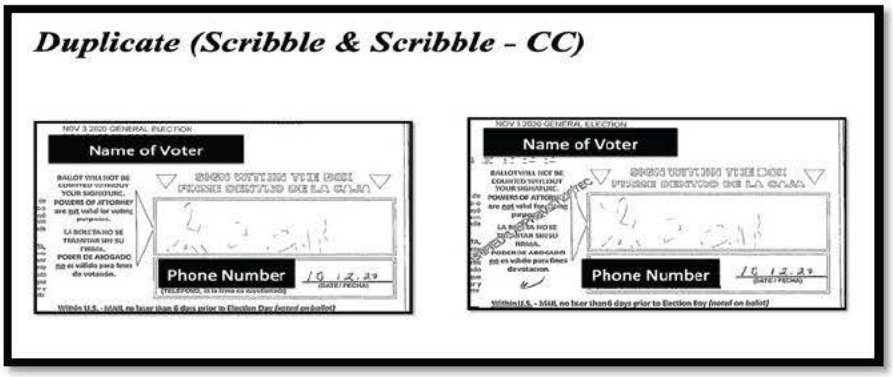


Figure 49: Scribble & Scribble Duplicate.

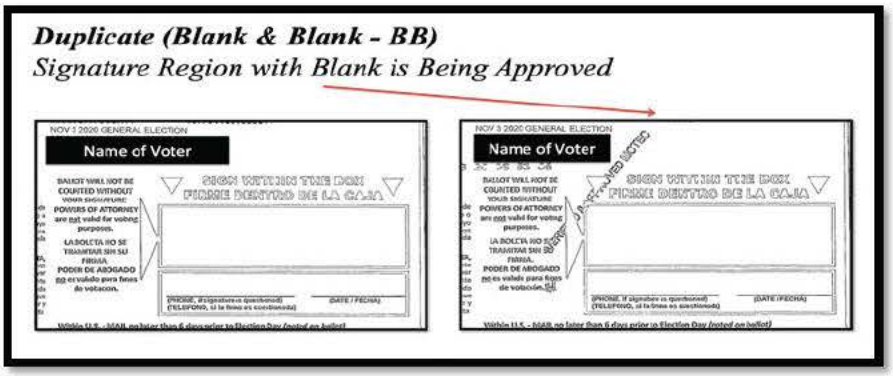


Figure 50: Blank & Blank Duplicate.

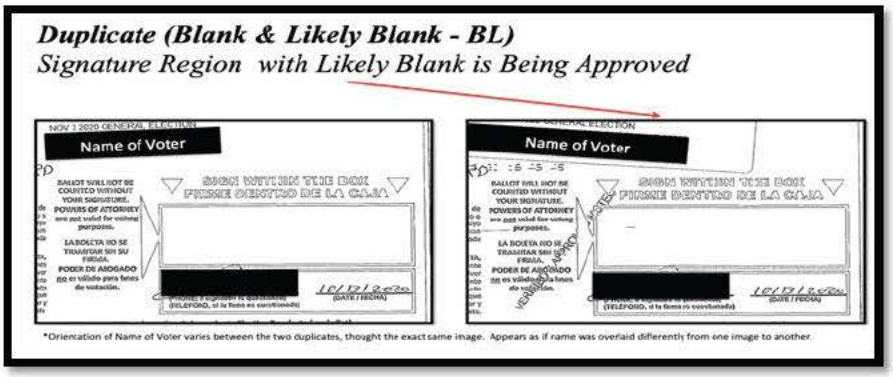


Figure 51: Blank & Likely Blank Duplicate.[24]

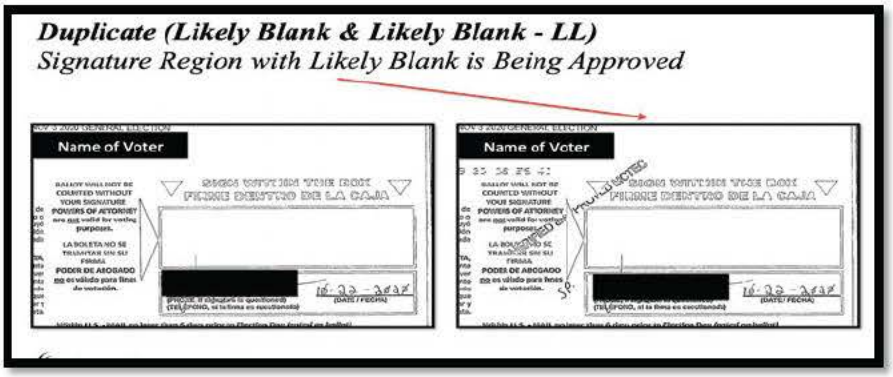


Figure 52: Likely Blank & Likely Blank Duplicate.

[24] Per the *Scope of Audit*, EchoMail solely analyzes the Signature Region. Herein, the Signature Region in the right image, by EchoMail, is classified as a Likely Blank, regardless of the voter placing their signature elsewhere, since non-white pixels of density 0%+ to 0.1% are within the Signature Region. During Signature Verification, reviewers resolve such issues when voters do not follow the explicit instructions, **"SIGN WITHIN THE BOX or FIRME DENTRO DE LA CAJA,"** through a process called adjudication.

SIGNATURE PRESENCE DETECTION RESULTS

There are a total of 1,929,240 EVB return envelope images received by EchoMail. EchoMail Signature Presence Detection was executed on all of these received images. Herein, the results of the EchoMail Analysis are presented. Of these, there are two groups. The first group is the set of 1,894,792 non-Duplicates. The second group is the set of 34,448, 2-Copy, 3-Copy, and 4-Copy Duplicates, as classified and tabulated in Table 5.

Classification of Non-Duplicate EVB Return Envelope Images

Concerning the first group of Non-Duplicates, EchoMail Signature Presence Detection produced the results shown in Table 7. 99.77% of the Non-Duplicate EVB return envelope images' Signature Regions were classified as having Signatures, 0.13% as Scribble, and 0.1% as Blank and Likely Blanks.

Classification of Non-Duplicate EVB Return Envelope Images	Count	Percentage
Signature	1,890,500	99.77%
Scribble	2,420	0.13%
Blank	1,771	0.09%
Likely Blank	101	0.01%
TOTAL	**1,894,792**	**100.00%**

Table 7: Non-Duplicate Signature Presence Detection Results.

Classification of Duplicate 2-Copy EVB Return Envelope Images

Concerning the second group, there are three sub-groups: 2-Copy Duplicates, 3-Copy

Duplicates, and 4-Copy Duplicates. Herein is provided the results of EchoMail Signature Presence Detection on the 33,868 2-Copy Duplicates. Table 8 summarizes the counts.

Image Copy I	Image Copy II	Classification	Count
Signature	Signature	SS	15,288
Signature	Blank	SB	1,348
Signature	Likely Blank	SL	26
Signature	Scribble	SC	72
Scribble	Blank	CB	6
Scribble	Likely Blank	CL	7
Scribble	Scribble	CC	142
Blank	Blank	BB	36
Blank	Likely Blank	BL	5
Likely Blank	Likely Blank	LL	4
		TOTAL	**16,934**

Table 8: 2-Copy Duplicate Signature Presence Detection Results.

Classification of Duplicate 3-Copy, 4-Copy EVB Return Envelope Images

Finally, of the Duplicates, the results of EchoMail Signature Presence Detection on the 564 3-Copy Duplicates, and 16 4-Copy Duplicates are presented in Table 9.

Type	Definitive Blanks	Likely Blanks	Scribbles	Signatures	Totals
3-Copy	40	2	16	506	**564**
4-Copy	2	0	0	14	**16**

Table 9: Three- & Four-Copy Duplicate Signature Presence Detection Results.

Table 10 provides the total number of Blanks e.g. "No Signatures" detected in the Signature Region that includes those Signature Regions categorized as Blank and Likely Blank.

	Blanks
Non-Duplicate Blanks	1,872
2-Copy Duplicate Blanks	45
3-Copy Duplicate Blanks	2
Total	1,919

Table 10: Total number of Signature Regions with Blanks.

Table 11 provides the total number of Scribbles detected in the Signature Region that includes those Signature Regions categorized as Scribble.

	Scribbles
Non-Duplicate Scribbles	2,420
2-Copy Duplicate Scribbles	155
3-Copy Duplicate Scribbles	5
Total	2,580

Table 11: Total number of Signature Regions with Scribbles.

SUMMARY OF ECHOMAIL ANALYSIS

Finally, Table 12 provides the consolidated results of EchoMail's Analysis integrating all the results of EchoMail Signature Presence Detection.

	EchoMail Analysis
EVB Return Envelope Images Received	1,929,240
Duplicate Analysis	
Duplicates	(17,322)
Unique EVB Return Envelopes	1,911,918
Signature Presence Detection	
No Signatures	(1,919)
Scribbles	(2,580)
EVBs Ready for Signature Verification	**1,907,419**

Table 12: Summary of results from EchoMail Analysis

EVB RETURN ENVELOPE IMAGES OF SCRIBBLES AND BLANKS

EchoMail delivered to the Arizona State Senate a USB flash drive containing the EVB return envelope images that the EchoMail Signature Presence Detection determined to be Blanks and Scribbles.

Name	Date Modified	Size	Kind
Manifest.txt	Today at 4:16 PM	694 bytes	Plain Text
NonDuplicateBlanks	Today at 4:02 PM	--	Folder
NonDuplicateScribbles	Today at 4:05 PM	--	Folder
ThreeCopyDuplicateBlanks	Today at 4:08 PM	--	Folder
ThreeCopyDuplicateScribbles	Today at 4:08 PM	--	Folder
TwoCopyDuplicateBlanks	Today at 4:08 PM	--	Folder
TwoCopyDuplicateScribbles	Today at 4:08 PM	--	Folder

Figure 53: Directory structure of USB flash drive delivered to Arizona State Senate containing the EVB return envelope images of Blanks and Scribbles per the SOW.

The directory structure of the USB flash drive sent to the Arizona State Senate is shown in Figure 53. The main directory contains a manifest of the files, with the filename "Manifest.txt." There are six (6) top-level directories as shown in Figure 53. Each top-level directory contains two (2) sub-directories names: FullImage and SignatureRegion. The FullImage sub-directory contains the original image received by EchoMail from the Arizona State Senate. The SignatureRegion sub-directory contains the portion of the Signature Region extracted by EchoMail from the original image.

Table 13 provides the breakdown of the files across the directories, and identifies which directories contain multiple versions of images in the case of 2-Copy and 3-Copy Duplicates. Table 13 indicates that there are a total of 9,426 files delivered to the Arizona State Senate on the USB flash drive containing the Blanks and Scribbles.

Directory Name	Full Image	Signature Region Image
Non-Duplicate Blanks	1872	1872
NonDuplicateScribbles	2420	2420
TwoCopyDuplicateBlanks	45 (2 versions)	45 (2 versions)
TwoCopyDuplicateScribbles	155 (2 versions)	155 (2 versions)
ThreeCopyDuplicateBlanks	2 (3 versions)	2 (3 versions)
ThreeCopyDuplicateScribbles	5 (3 versions)	5 (3 versions)

Table 13: The breakdown of the 9,426 image files containing Blanks and Scribbles delivered to the Arizona State Senate on the USB flash drive.

GLOBAL TEMPORAL SIGNALS ANALYSIS

In Table 14, are the results of ordering the 1,919,598 SIF, EVB return envelope images, by the date stamp on the batches of EVB return envelope images provided to EchoMail.

Date	EVBRE	Blanks	Blanks%	Scribbles	Scribbles%	Duplicates	Duplicates%
10/9/20	5454	6	0.1100%	4	0.0733%	13	0.2384%
10/10/20	27978	90	0.3217%	34	0.1215%	291	1.0401%
10/12/20	45203	144	0.3186%	41	0.0907%	347	0.7676%
10/13/20	28453	46	0.1617%	43	0.1511%	237	0.8330%
10/14/20	190517	640	0.3359%	236	0.1239%	2079	1.0912%
10/15/20	126004	383	0.3040%	163	0.1294%	1392	1.1047%
10/16/20	97118	295	0.3038%	138	0.1421%	1131	1.1646%
10/17/20	80924	183	0.2261%	105	0.1298%	779	0.9626%
10/18/20	43185	121	0.2802%	65	0.1505%	567	1.3130%
10/19/20	2778	2	0.0720%	5	0.1800%	272	9.7912%
10/20/20	121404	242	0.1993%	173	0.1425%	1599	1.3171%
10/21/20	93313	193	0.2068%	136	0.1457%	1269	1.3599%
10/22/20	76339	177	0.2319%	119	0.1559%	932	1.2209%
10/23/20	76053	148	0.1946%	104	0.1367%	1577	2.0736%
10/24/20	80451	80	0.0994%	105	0.1305%	976	1.2132%
10/25/20	62768	63	0.1004%	71	0.1131%	916	1.4593%
10/26/20	7053	8	0.1134%	17	0.2410%	341	4.8348%
10/27/20	105905	97	0.0916%	185	0.1747%	1086	1.0254%
10/28/20	116391	115	0.0988%	148	0.1272%	1982	1.7029%
10/29/20	84920	80	0.0942%	151	0.1778%	1182	1.3919%
10/30/20	69062	55	0.0796%	104	0.1506%	1295	1.8751%
10/31/20	63356	36	0.0568%	90	0.1421%	999	1.5768%
11/1/20	67120	39	0.0581%	127	0.1892%	1860	2.7712%
11/2/20	16377	22	0.1343%	50	0.3053%	1332	8.1334%
11/3/20	67170	28	0.0417%	118	0.1757%	2197	3.2708%
11/4/20	157904	82	0.0519%	232	0.1469%	3392	2.1481%
11/5/20	1874	5	0.2668%	13	0.6937%	1595	85.1121%
11/6/20	2380	7	0.2941%	12	0.5042%	744	31.2605%
11/7/20	1512	2	0.1323%	10	0.6614%	1459	96.4947%
11/9/20	632	4	0.6329%	6	0.9494%	607	96.0443%
Total	**1919598**	**3393**	**0.1768%**	**2805**	**0.1461%**	**34448**	**1.79%**

Table 14: SIF's by Date, EVBRE, EVBRE%, and Count and Percentage of Blanks, Scribbles, and Duplicates.

The total number of SIF's in Table 14 represents 99.5% all EVB return envelopes (as previously reported in Table 4). This analysis does not include the 9,642 UIF's, LIF and BIF EVB return envelope images. Column 2 denoted by "EVBRE" is the EVB return envelope images per day. The date is assumed, for the purpose of this discussion, to represent the day on which Maricopa officials received the EVB return envelope images

(below in the *Questions* section, one of the inquiries to Maricopa officials is to confirm this assumption). Columns 3, 5, and 7, are the total number of Blanks, Scribbles, and Duplicates, received for that Date, respectively. Columns 4, 6, and 8 are the percentage of Blanks, Scribbles, and Duplicates, as a function of the total number of daily EVBRE's, respectively.

Control Signal – Plot of EVBRE by Day

In Figure 54, a graph of the EVBRE by day is provided. This plot serves as a control signal for subsequent comparisons.

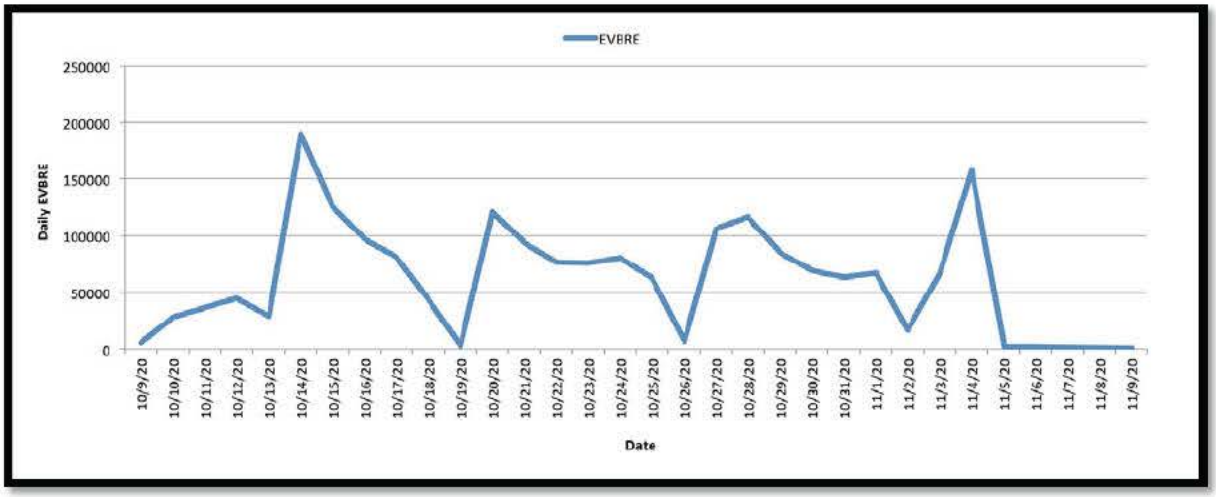


Figure 54: Daily EVB Return Envelope Images (EVBRE).

Daily EVBRE Compared to Daily Blanks, Scribbles, and Duplicates

In Figure 55, the daily EVBRE is plotted using a scale on the right y-axis, along with the Blanks, Scribbles, and Duplicates by day with a different scale on the left y-axis. This graph provides a visualization of the daily Blanks, Scribbles, and Duplicates as compared

to the control signal of the daily EVBRE. It appears, based on the scaling, the Blanks and the Scribbles correlate with the EVBRE daily trends. However, the daily Duplicates signal appears to diverge from the control signal at various points.

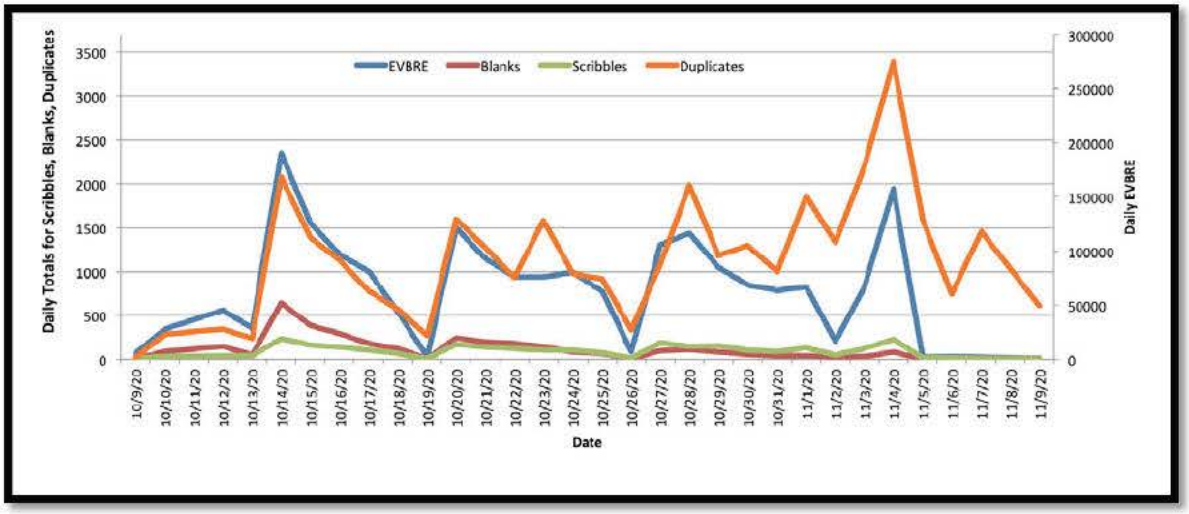


Figure 55: Daily EVB Return Envelope Images (EVBRE) Compared to Daily Blanks, Scribbles, and Duplicates.

Daily EVBRE Comparison to Daily Duplicates as % of Daily EVBRE

To investigate more closely the daily Duplicates relative to daily EVBRE, a signal is developed that plots the daily Duplicate counts as a percentage of the daily EVBRE. This signal is shown alongside the daily EVBRE using two different scales in Figure 56. The left y-axis is used to plot daily Duplicates as a percentage of daily EVBRE, while the right y-axis is used to plot the daily EVBRE. The graph reveals a significant surge of 7,797 Duplicates during the six days from 11/04/2020 to 11/09/2020.

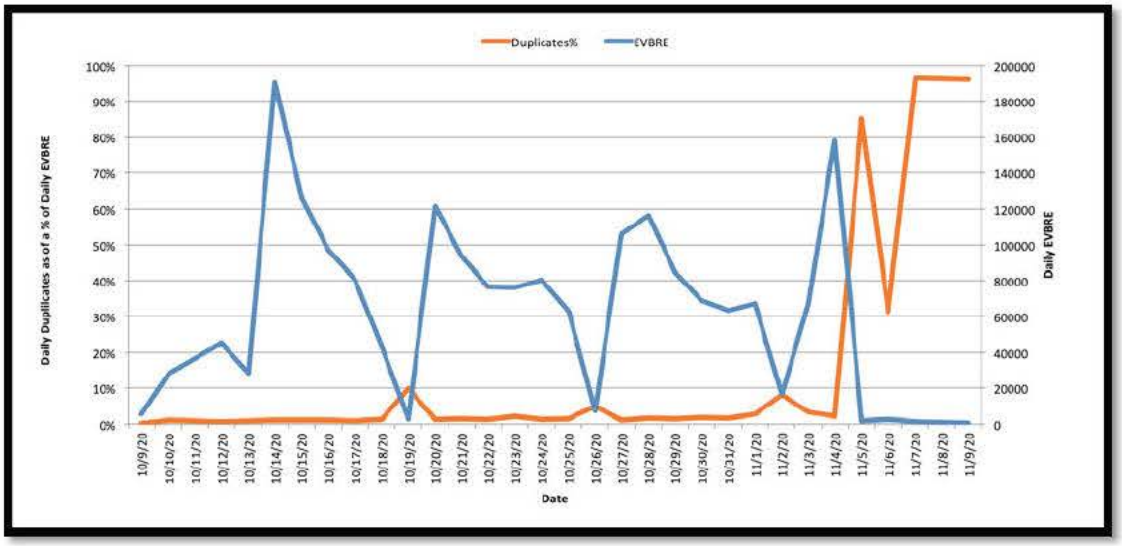


Figure 56: Daily EVB Return Envelope Images (EVBRE) Compared to Daily Duplicates as a Percentage of Daily EVBRE.

This count of Duplicates represents 22.6% of the total number of 34,448 Duplicates for the entire election. Moreover, here are other observations from the graph in Figure 56:

- On 10/19/2020, the daily Duplicate percentage of EVBRE has a local maxima while the daily EVBRE has a local minima.
- Similarly, on 10/26/2020, the daily Duplicate percentage of EVBRE has a local maxima while the daily EVBRE has a local minima.
- Similarly, on 11/02/2020, the daily Duplicate percentage of EVBRE has local a maxima while the daily EVBRE has a minima.
- On 11/05/2020, over 85% of the daily EVBRE are Duplicates
- For the two (2) days, on 11/07/2020 and on 11/09/2020, over 96% of the daily EVBRE are Duplicates.
- On the days of 11/05/2020, 11/07/2020, and 11/09/2020, the daily Duplicates

percentage is nine to ten times more than the highest previous daily Duplicate percentage recorded on 10/19/2020.

Daily EVBRE Compared to Daily Blanks, Scribbles as % of Daily EVBRE

The above investigation of daily Duplicates as a percentage of daily EVBRE motivated a closer investigation of the daily Blanks and Scribbles as a percentage of daily EVBRE.

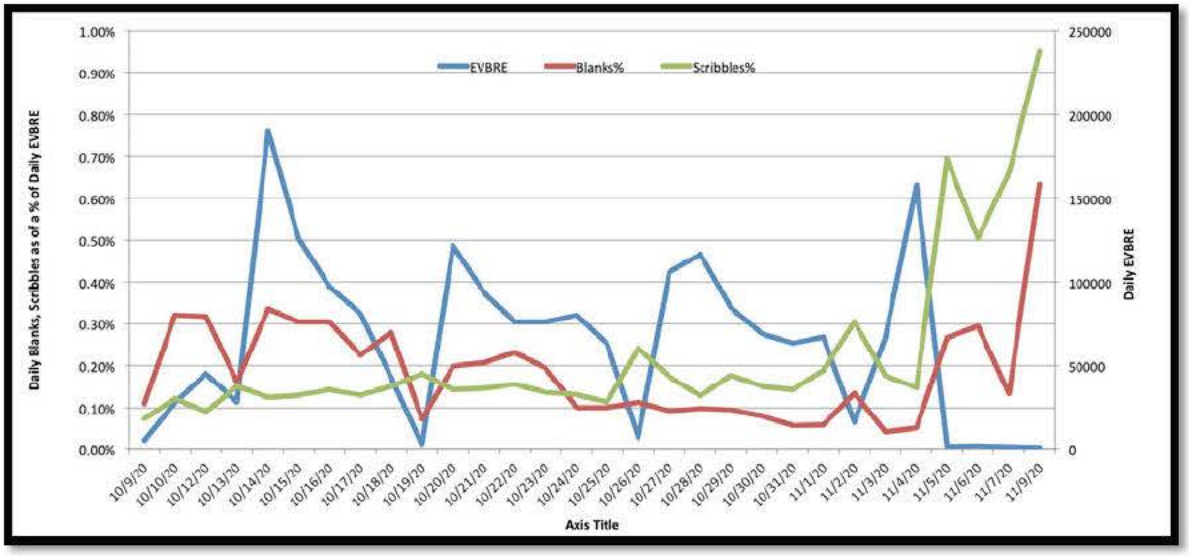


Figure 57: Daily EVBRE Compared to Daily Duplicates as a Percentage of Daily EVBRE.

In Figure 57, a signal is developed that plots the daily Blanks and Scribbles as a percentage of the daily EVBRE. This signal is shown alongside the daily EVBRE using two different scales in Figure 57. The left y-axis is used to plot daily Blanks and Scribbles as a percentage of daily EVBRE, while the right y-axis is used to plot the daily EVBRE. Though the numbers of Blanks and Scribbles are relative small, the graph reveals a similar pattern to the increase in daily Duplicates, shown in Figure 53 during the period of 11/04/2020 to 11/09/2020.

SUPERVISED IMAGE REVIEW

The above temporal results motivated a supervised (human review) of a sample of the Duplicates, and various images. Below are examples of some significant anomalies.

Duplicate Blanks Stamped and Approved

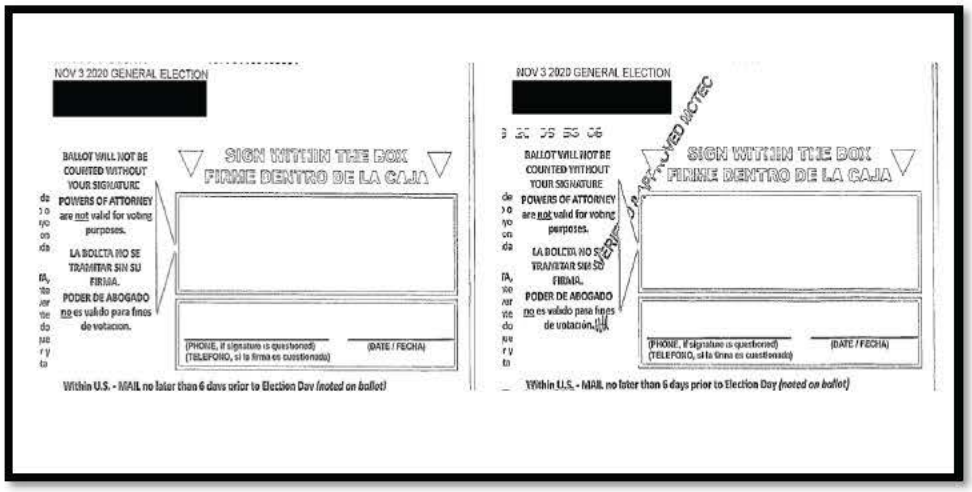


Figure 58: #1: Blank Duplicate being STAMPED: VERIFIED & APPROVED MCTEC.

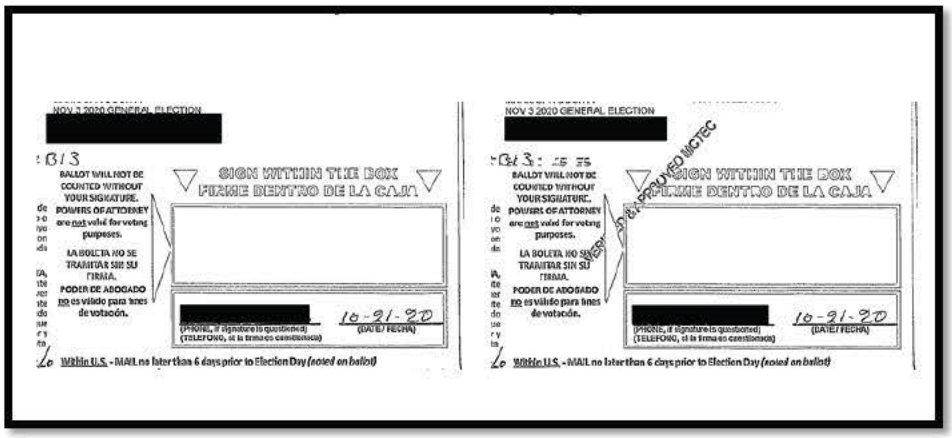


Figure 59: #2: Blank Duplicate being STAMPED: VERIFIED & APPROVED MCTEC.

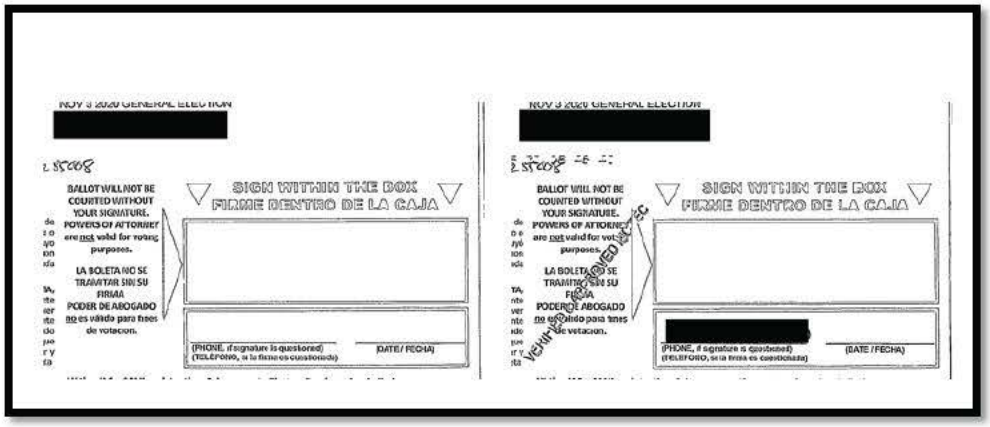


Figure 60: #3: Blank Duplicate being STAMPED: VERIFIED & APPROVED MCTEC.

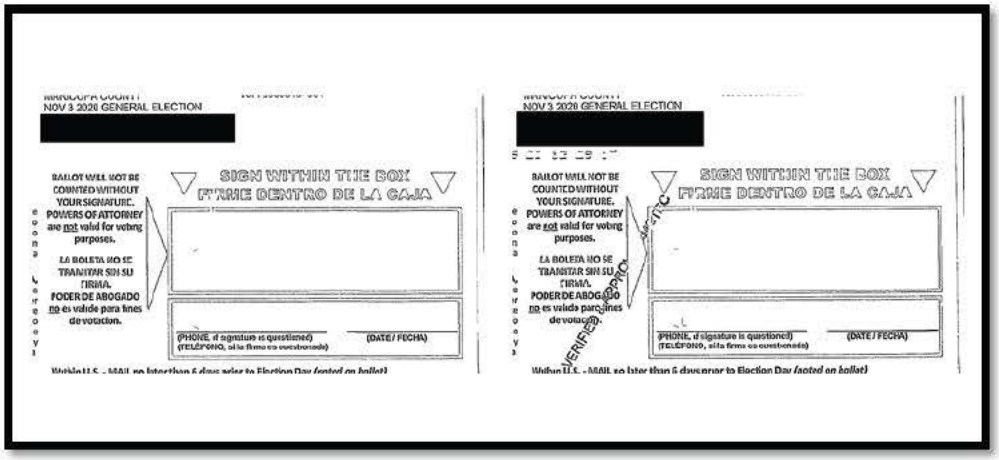


Figure 61: #4: Blank Duplicate being STAMPED: VERIFIED & APPROVED MCTEC.

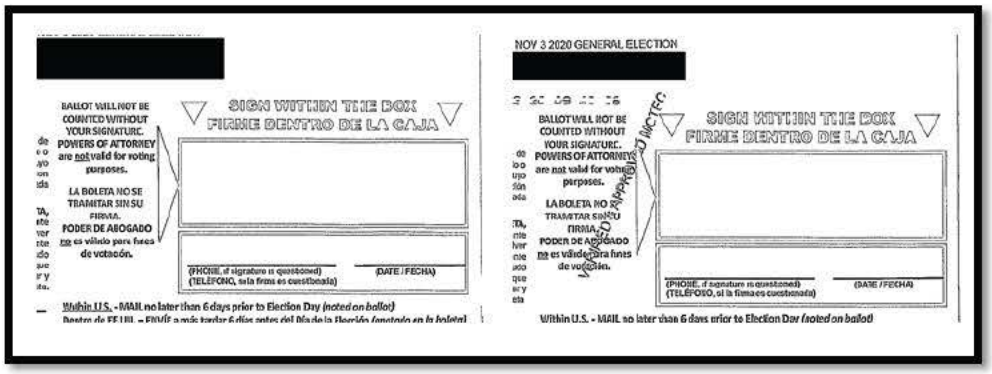


Figure 62: #5: Blank Duplicate being STAMPED: VERIFIED & APPROVED MCTEC.

Stamped in Signature Region (Non-Duplicates, Two per image)

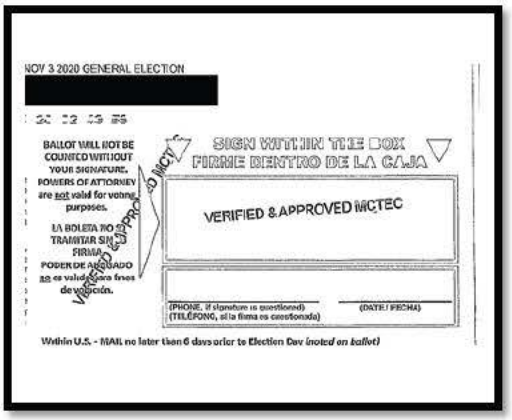


Figure 63: #1: Non-Duplicate VERIFIED & APPROVED MCTEC in Signature Region.

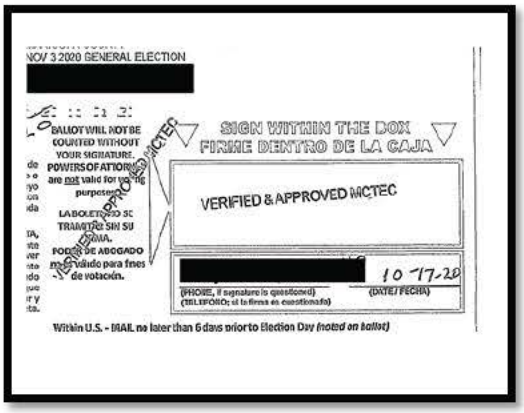


Figure 64: #2: Non-Duplicate VERIFIED & APPROVED MCTEC in Signature Region.

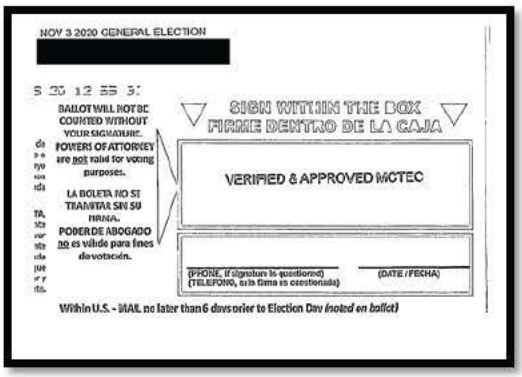


Figure 65: #3: Non-Duplicate VERIFIED & APPROVED MCTEC in Signature Region.

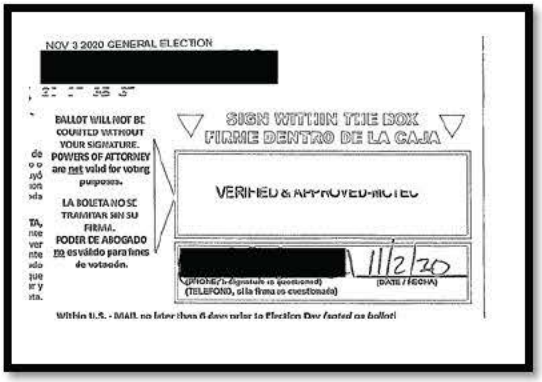


Figure 66: #4: Non-Duplicate VERIFIED & APPROVED MCTEC in Signature Region.

3-Copy Duplicate Blanks Stamped and Approved

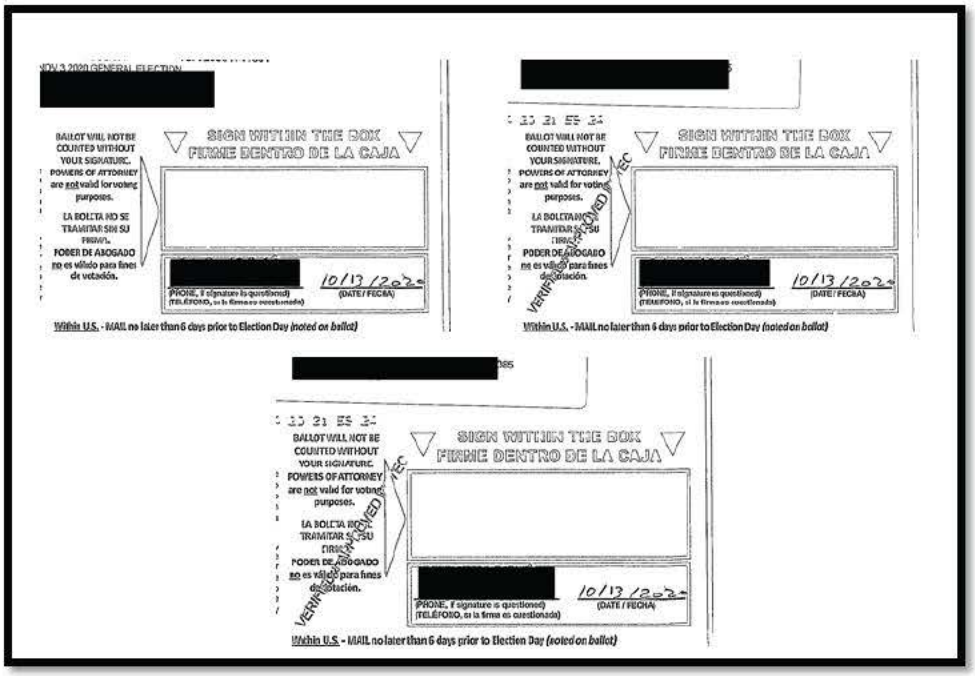


Figure 67: #1: 3-Copy Duplicate Blank being VERIFIED & APPROVED MCTEC.

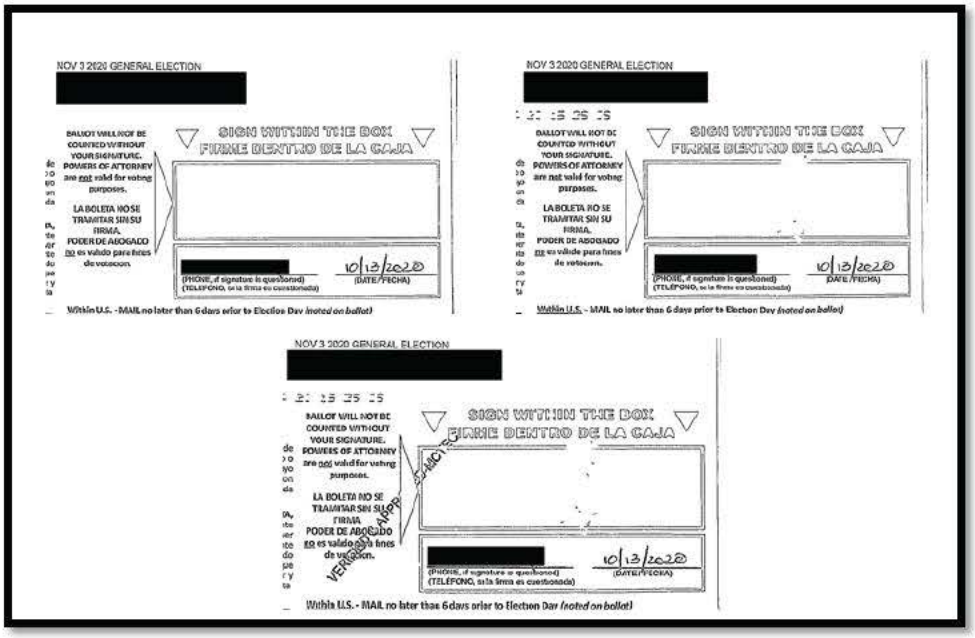


Figure 68: #2: 3-Copy Duplicate Blank being VERIFIED & APPROVED MCTEC.

3-Copy Duplicate Scribbles Stamped and Approved.

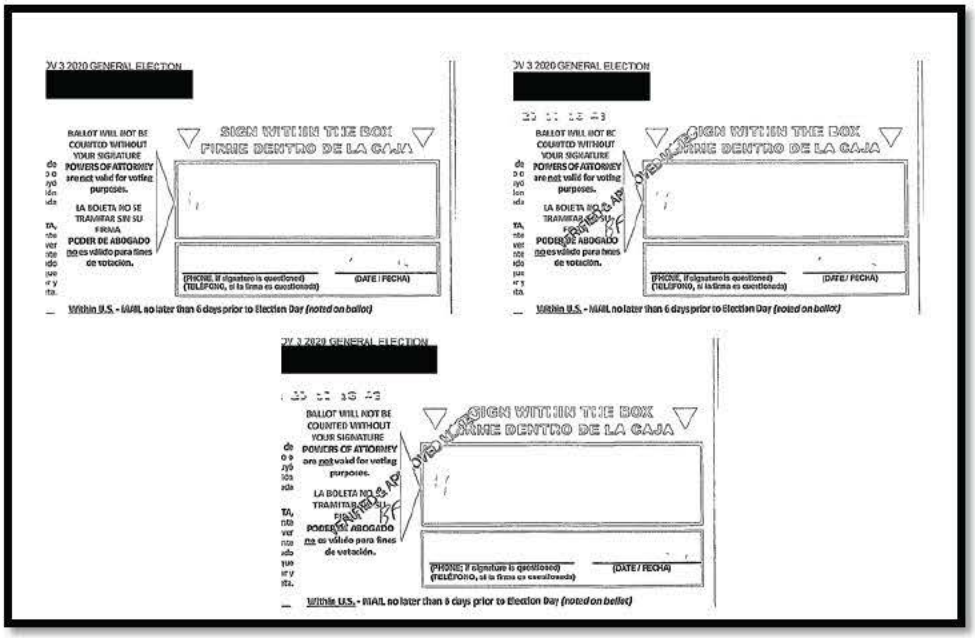


Figure 69: #1: 3-Copy Duplicate Scribble being VERIFIED & APPROVED MCTEC.

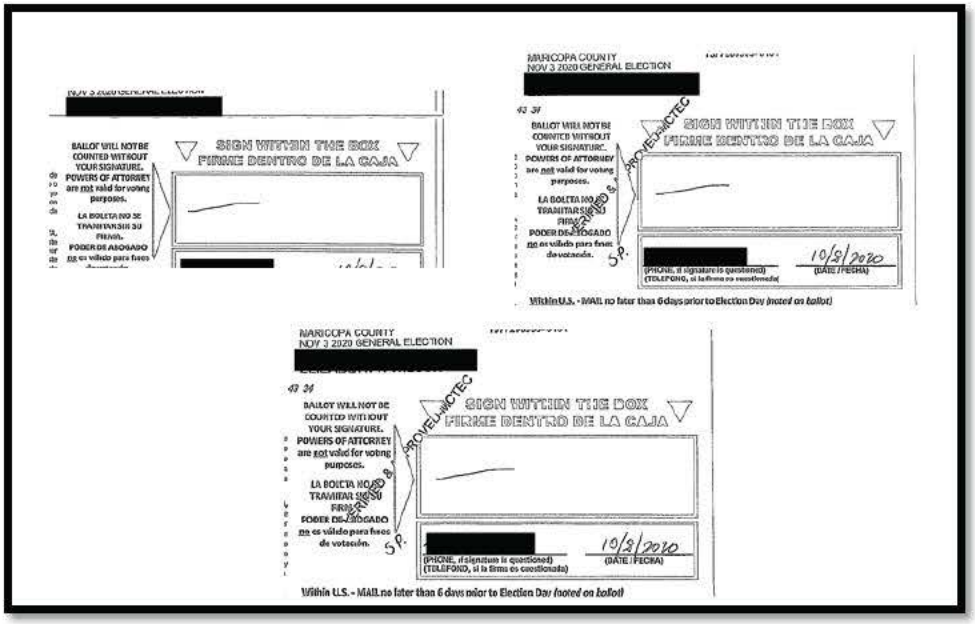


Figure 70: #2: 3-Copy Duplicate Scribble being VERIFIED & APPROVED MCTEC.

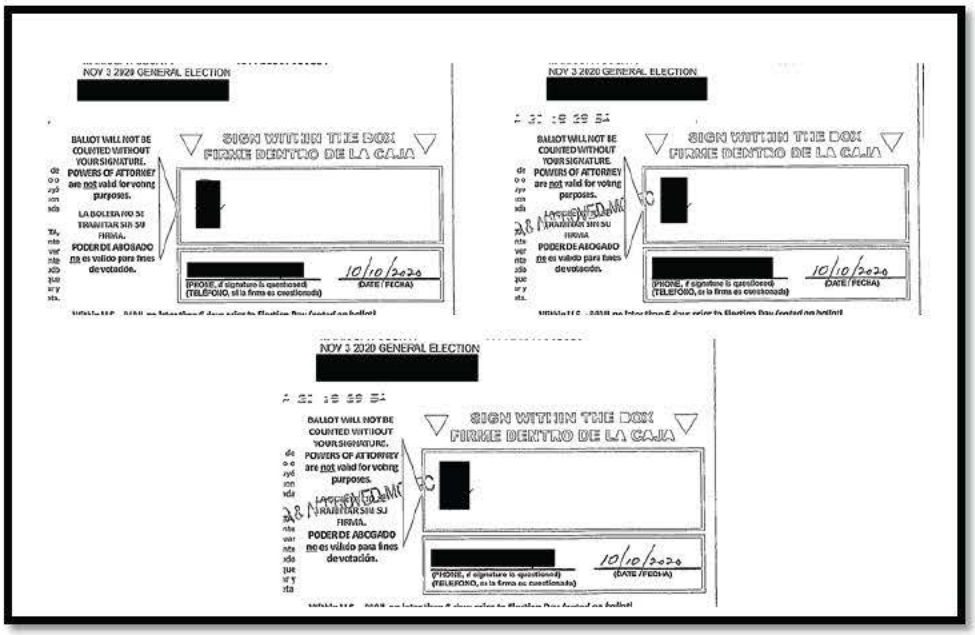


Figure 71: #3: 3-Copy Duplicate Scribble being VERIFIED & APPROVED MCTEC.

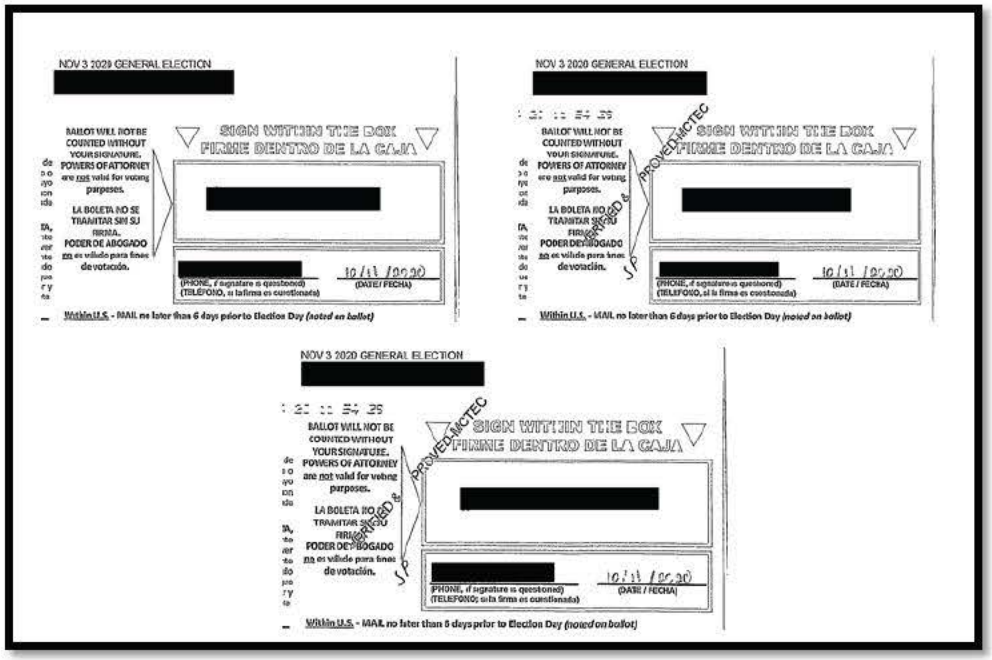


Figure 72: #4: 3-Copy Duplicate Scribble being VERIFIED & APPROVED MCTEC.

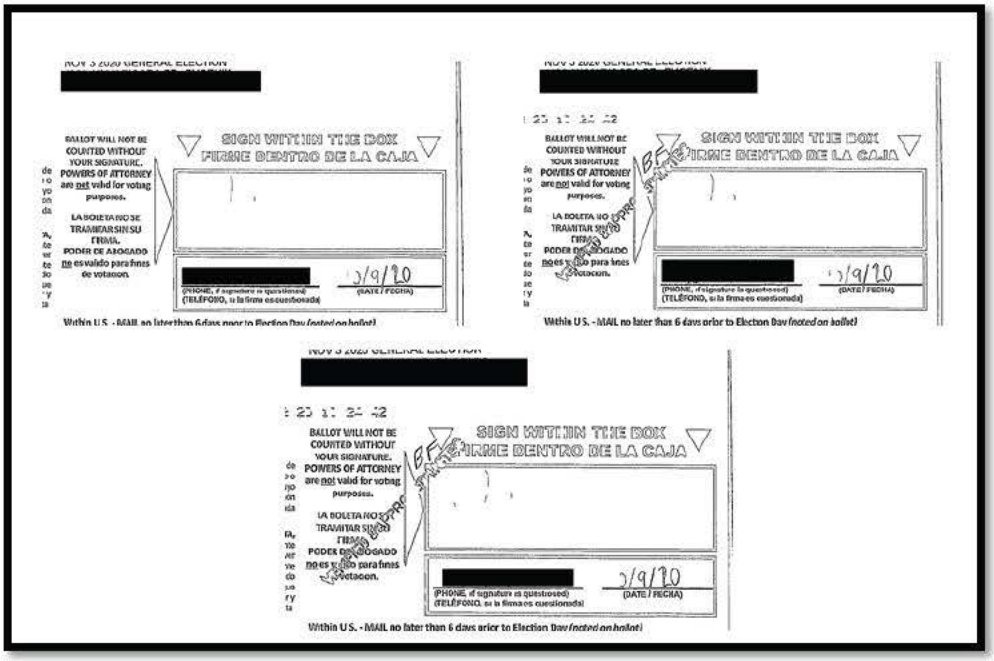


Figure 73: #5: 3-Copy Duplicate Scribble being VERIFIED & APPROVED MCTEC.

"VERIFIED & APPROVED STAMP" BEHIND Envelope Triangle

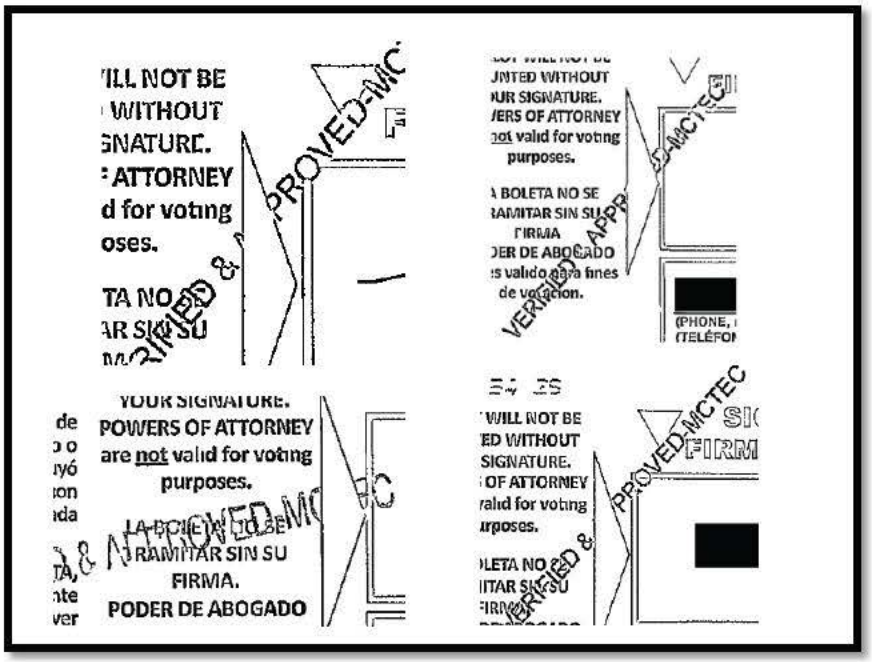


Figure 74: #1: VERIFIED & APPROVED MCTEC Behind Triangle

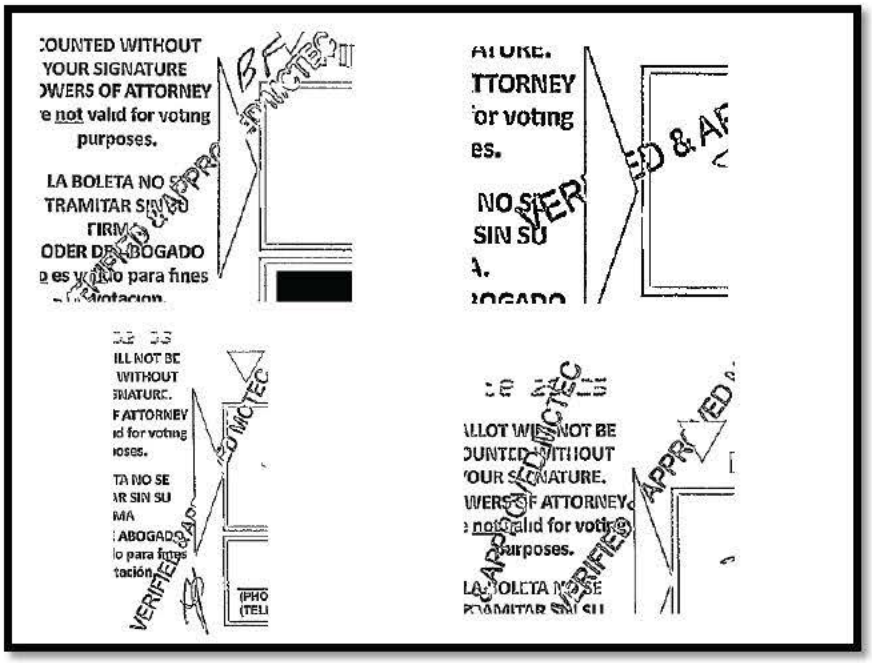


Figure 75: #2: VERIFIED & APPROVED MCTEC Behind Triangle.

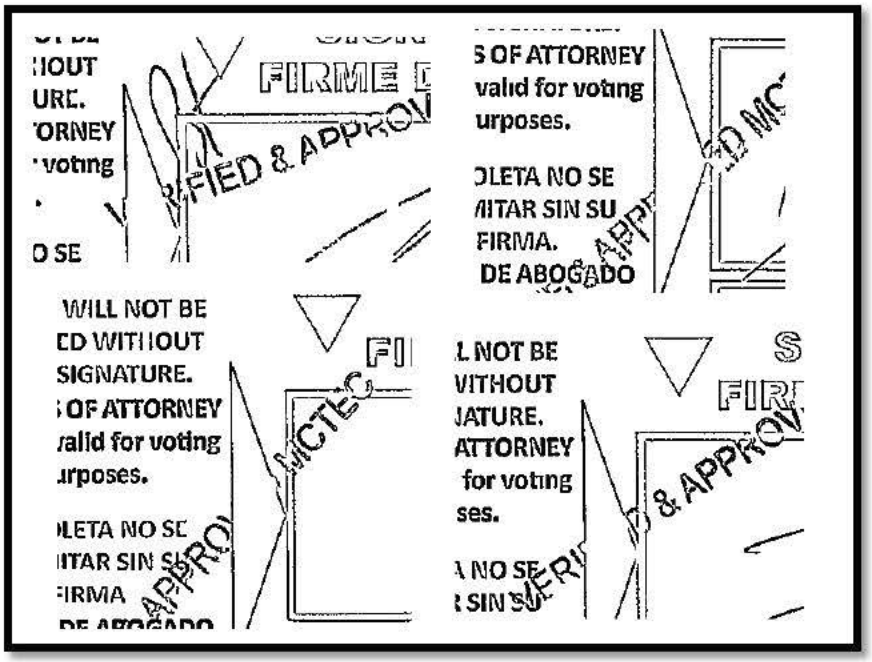


Figure 76: #3: VERIFIED & APPROVED MCTEC Behind Triangle.

Same Name, Same Signature, Same Phone, Two Different Voter-IDs

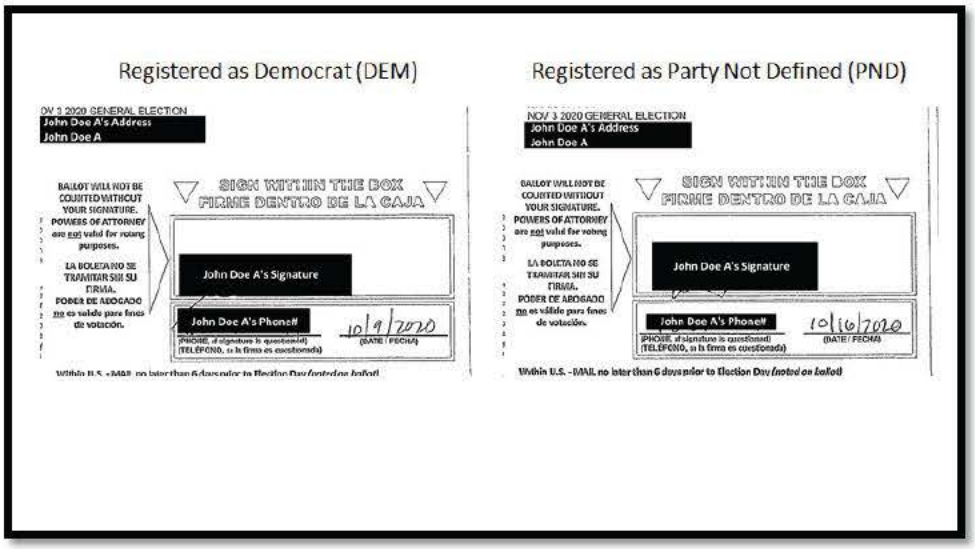


Figure 77: #1: Same Name, Same Signature, Same Phone, Two Different Voter-IDs

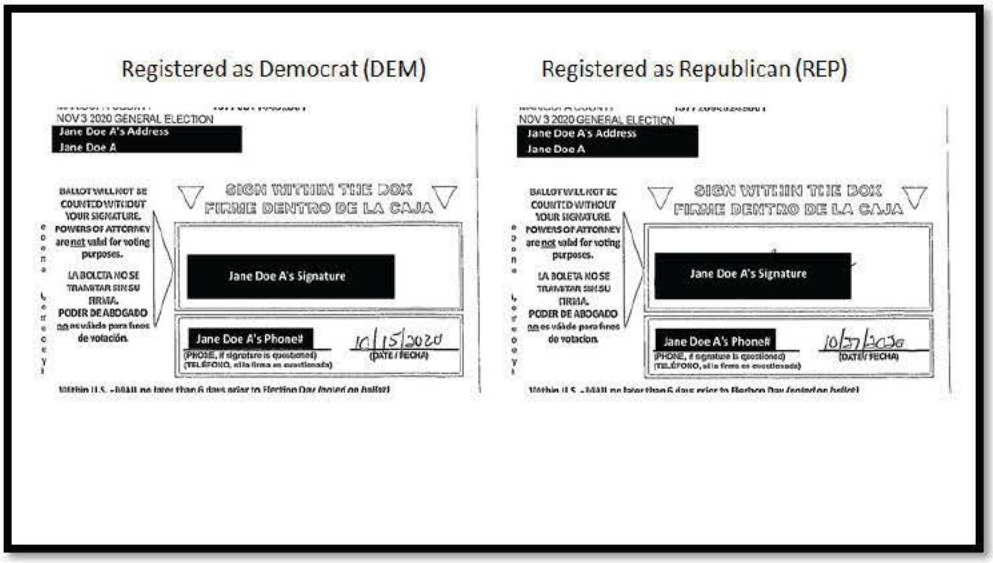


Figure 78: #2: Same Name, Same Signature, Same Phone, Two Different Voter-IDs

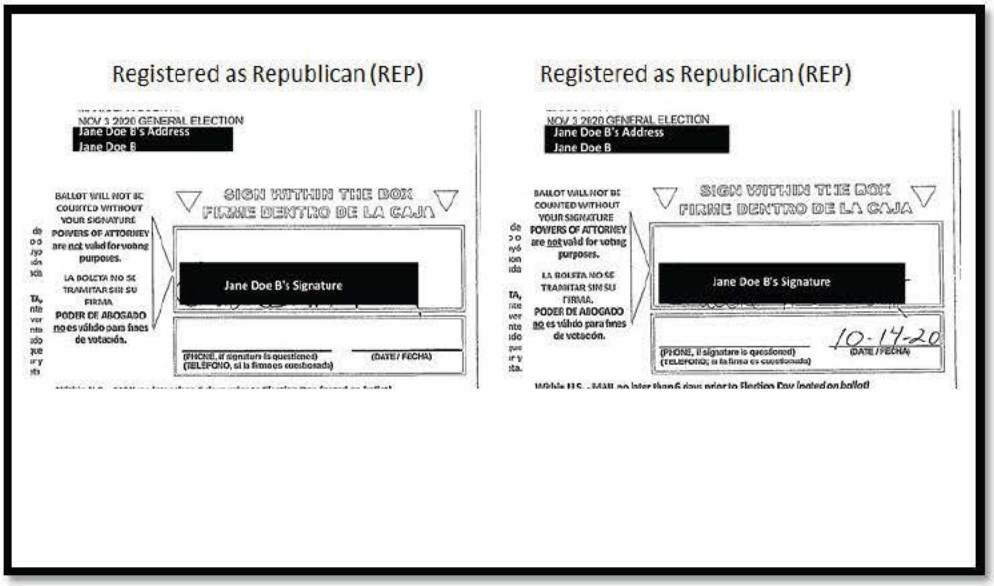


Figure 79: #3: Same Name, Same Signature, Same Phone, Two Different Voter-IDs

DISCUSSSION

The discussion herein provides a comparative analysis of EchoMail results with Maricopa; offers questions for Maricopa election officials; and, proposes future research.

COMPARATIVE ANALYSIS

	EchoMail Analysis	Maricopa Reported	Variance
EVB Return Envelopes Received	**1,929,240***	***Unknown***	**NA**
Duplicate Analysis			
Duplicates[25]	(17,322)	*Un-reported*	NA
Unique EVB Return Envelopes	**1,911,918**	**1,918,463****	**(6,545)**
Signature Presence Detection			
No Signature Ballots[26]	(1,919)	(1,455)	(464)
Scribbles[27]	(2,580)	NA	(2580)
EVBs Ready for Signature Verification	**1,907,419**	**1,917,008**	**(9,589)**
Signature Verification			
"Bad Signatures"	NA	(587)	NA
"Late Returns"	NA	(934)	NA
Total EVBs Verified and Counted	**NA**	**1,915,487**	**NA**

Table 15: Summary report of EchoMail Analysis of EVB return envelope images compared with Maricopa's results reported in November General Election *CANVASS* report.

*This the total count of all EVB return envelope images received by EchoMail from Arizona State Senate.
**This count is all EVB return envelopes verified and counted by Maricopa (1,915,487) plus those classified by Maricopa as "No Signatures" (1455), "Bad Signatures" (587), and "Late Returns" (934), as documented in Maricopa County's November 2020 *CANVASS* report.

[25] In the EchoMail Analysis, those EVB return envelope images with same image file name were deemed "Duplicates." The EVB return envelope image file names are voter specific. 17,126 unique voters submitted 34,448 2-copy, 3-copy, 4-copy duplicate ballots. The *CANVASS* report filed by Maricopa election officials did not report Duplicates.

[26] "No Signature Ballots" in EchoMail Analysis are those Signature Regions on EVB return envelope images classified to be "Blanks" based on a non-white pixel density of 0%, and "Likely Blanks" based on a non-white pixel density between 0%+ to 0.1%.

[27] "Scribbles" in EchoMail Analysis are those EVB return envelope images containing likely illegible signatures in the Signature Region, wherein a scribble is defined as a Signature Region containing a non-white pixel density between 0.1%+ to 1%.

Based on the results in Table 15, here is the summary of findings:

- **It is unknown, per the *CANVASS* report, how many EVB return envelopes were *originally* received by Maricopa election officials.** EchoMail received a data set of 1,929,240 EVB return envelope images that were represented to EchoMail as being the set of *all* EVB return envelopes originally received by Maricopa. However, the *CANVASS* report does not document how many EVB return envelopes were originally received Maricopa election officials.[28]

- **EchoMail identified 34,448 EVB return envelope images being 2-Copy, 3-Copy and 4-Copy Duplicates** originating from 17,126 unique voters, while no Duplicates were reported in Maricopa's *CANVASS* report.[29]

- 6,545 ***more*** unique EVB return envelopes were processed by Maricopa than identified by EchoMail.

- 464 ***more*** "No Signature" EVB return envelopes were reported by EchoMail. EchoMail identified 1,919 EVB return envelope images with Blank or Likely Blank in the Signature Region i.e. "No Signature." Maricopa reported 1,455 "No Signature" EVB return envelopes.

- 2,580 Scribbles identified by EchoMail in the Signature Region of EVB return envelope images. A "Scribble" is when a Signature Region on an EVB return

[28]All EVBs reported that were received by Maricopa are assumed to have been accompanied by return envelopes or affidavits with signatures.
[29]The 2020 November General Election *CANVASS* report does not mention Duplicates. A search of the keyword "duplicate" reveals no instances in the *CANVASS* report.

envelope image contains a non-white pixel density between 0.1%+ to 1%, and may indicate a potential "Bad Signature." EchoMail was not commissioned with the task of performing Signature Verification.

- Maricopa reported 587 "Bad Signatures," which is 0.031% of the total EVB return envelopes received by Maricopa. Though EchoMail was not commissioned to perform Signature Verification, if EchoMail's identification of 2,580 Scribbles were all designated as "Bad Signatures," that would be 0.134% of Maricopa's total EVB return envelopes received. This percentage is at least four times more than the "Bad Signatures" percentage reported by Maricopa.

- While the number of EVB returns envelopes in Maricopa for the 2016 general election ***increased*** from 1,257,179 to 1,918,463 EVB return envelopes for the 2020 general election, representing a 52.6% ***increase*** (or by 661,284 EVB return envelopes), the number of rejections from Signature Mismatches of EVB return envelopes, from 2016 to 2020, ***decreased*** by 59.7%. This inverse relationship requires explanation.

- 9,589 ***more*** EVB return envelopes were submitted for Signature Verification by Maricopa than the EVB return envelope images identified by EchoMail as having signatures.

- A full audit of Maricopa's Signature Verification process is necessary, and can be accomplished by comparing each signature on EVB return envelope images with an

image of the voter's signature from voter registration files. This will provide a quantitative metric to assess confidence level of Signature Verification.

- Disclosure of Maricopa's Standard Operating Procedure (SOP) for EVB processing, Chain of Custody, and Signature Verification methods, including the SOP and methodology for curing questionable signatures, is necessary.

QUESTIONS FOR MARICOPA ELECTION OFFICIALS

- Did Maricopa County receive any duplicate EVBs?
  - EchoMail identified 34,448 EVB return envelope images being 2-copy, 3-copy and 4-copy Duplicates originating from 17,126 unique voters, while no Duplicates were reported in Maricopa's *CANVASS* report

- Is the reason that EchoMail has ***more*** "No Signatures" than reported by Maricopa because EchoMail analyzed solely the Signature Region? If not, why?
  - EchoMail identified 1,919 Blanks in Signature Region of EVB return envelopes
  - Maricopa reported 1,455 "No Signatures" in EVB return envelopes

- Why did EchoMail detect more Scribbles than Maricopa's reporting of "Bad Signatures"?
  - EchoMail identified 2,580 Scribbles in Signature Region of EVB return envelopes
  - Maricopa reported 587 "Bad Signatures" from its Signature Verification
  - Had EchoMail been commissioned to identify "Bad Signatures," at least 2,580 Scribbles would have been classified as "Bad Signatures;" 1,993 more "Bad Signatures" than the 587 identified by Maricopa

- Are the date stamps on the directories for SIFs, in the data set provided to EchoMail, the date in which the Maricopa election officials received the EVB return envelopes?

- Why does the approval stamp, ***"VERIFIED & APPROVED MCTEC"*** appear to exist only on a relatively small subset of EVB return envelopes?

- Did Maricopa stamp some EVB return envelopes as ***"VERIFIED & APPROVED MCTEC"*** **even though Signature Region is blank**, since they found a signature elsewhere i.e. outside of the Signature Region, during Signature Verification?

- What is the Standard Operating Procedure ("SOP") for the EVB processing?

- What is the SOP for Signature Verification and curing of questionable signatures?

- What is the Chain of Custody for EVB return envelopes?

- Why is the surge in Duplicates (and Blanks and Scribbles) during 11/04/2020 to 11/09/2020 incongruent with the trend of EVBRE daily counts during the same period?

- Why is the ***"VERIFIED & APPROVED MCTEC"*** stamp appearing "behind" the printed envelope triangle?
- Can Two Voter-IDs be associated with the same person at the same address with matching signatures?
- Why are Blanks being stamped as ***"VERIFIED & APPROVED MCTEC?"***
- Why is the stamp ***"VERIFIED & APPROVED MCTEC"*** appearing in a blank Signature Region?

FUTURE RESEARCH

This audit has identified various anomalies and discrepancies enumerated above. Though the scope of this audit, as repeatedly clarified, was not to perform Signature Verification, a random sampling of over 200 signatures, 4-weeks before the 2020 Election Day and 4-days after Election Day, are shown in Figures 58 and 59, respectively.

Figure 58: Random selection of signatures from 4-weeks before Election Day. Approximately 3% appear as "Illegible" signatures, while approximately 97% appear as "Legible" signatures.

Figure 59: Random selection of signatures from 4-days ***after*** Election Day. Approximately 97% appear are "Illegible" signatures while approximately 3% appear as "Legible" signatures.

It is unclear what percentage of the signatures in Figure 58 versus those in Figure 59 were considered "Bad Signatures" or the signatures that required curing by Maricopa election officials. Of the ones in Figure 58, 4-weeks ***before*** Election Day, approximately 3% appear as "Illegible" signatures while approximately 97% appear as "Legible" signatures. Alternatively, of the ones in Figure 59, 4-days ***after*** Election Day, approximately 97% appear are "Illegible" signatures while approximately 3% appear as "Legible" signatures. Observations such as these, along with the discrepancies and anomalies identified from this audit suggest the following be considered for future research:

- Full systems analysis of the efficacy of Maricopa's Signature Verification process, which can be accomplished by comparing all signatures on EVB return envelope images with image of signatures from voter registration files. This can lead to a quantitative metric to assess confidence level of Signature Verification. The following next steps can be pursued in this effort:
  - Acquire Maricopa County's SOP for signature verification
  - Acquire Maricopa County's 27-point analysis algorithm for signature comparison
  - Replicate signature verification process to scientifically calculate false positives, false negatives, and error rate to determine a true confidence value of the signature verification of EVBs

- Disclosure of Maricopa's Standard Operating Procedure (SOP) for EVB processing, Chain of Custody, and Signature Verification methods, including the SOP and methodology for curing questionable signatures.

CONCLUSION

Based on an engineering systems approach employing pattern recognition classification methods, this audit has delivered a comprehensive analysis of the Signature Region of the Early Voting Ballot (EVB) return envelope images, from Maricopa's November 2020 Election. The objective of this audit was to perform an analysis of these images to determine the counts of Signatures, Blanks, and Scribbles on the EVB return envelope images, and to compare these counts with the counts as reported in the *November General Election CANVASS* report by Maricopa County election officials.

This objective has been accomplished; however, the discussion herein has also aimed to motivate a grander objective: to inspire the reader to move beyond partisanship, vitriol, and controversy to appreciate the need for an *engineering systems approach*, particularly in the modern era of the 21st century, where complex engineering systems pervade every aspect of human existence. Our voting systems are complex engineering systems. Our ability to move beyond left and right and to appreciate the nature of these systems – interconnected systems of systems that serve a diversity of stakeholders – is critical to advancing the systems integrity of U.S. election processes.

This audit has uncovered anomalies in the EVB systems processes that provide all stakeholders a historic opportunity to address and resolve these issues with an engineering systems mindset: to discover the root cause, find the real solution, implement the solution, and monitor the systems ongoing performance.

Below, in Table 16, is an itemized list of the anomalies uncovered. Each anomaly is prefaced by a particular *engineering systems property* or "ility" that can be enhanced if the anomaly is addressed.

System Property ("ility")	Anomaly	Pages
Transparency	There is a lack of visibility of how many EVB return envelopes were received by the Maricopa election officials. EchoMail shared that it had received a total of **1,929,240** EVB return envelope images. However, it is not clear how many EVB return envelopes were received by Maricopa.	p. 62
Verifiability	EchoMail's analysis revealed that 17,126 unique voters submitted 34,448 2-copy, 3-copy, and 4-copy Duplicates of EVB return envelopes. However, the *CANVASS* report's lack of disclosure on the number of Duplicates processed, does not allow for an immediate verification of this audit's Duplicates' count.	p. 63
Auditability and Chain of Custody	EchoMail identified ten (10) different kinds of 2-Copy Duplicate classifications, and provided their examples. What emerges from these examples is a lack of clarity on why one copy was stamped **"VERIFIED AND APPROVED MCTEC"** and why the other was not. If adjudication took place, is there a communications record of which reviewer contacted the voter and how the matter was resolved?	pp. 64-67
Reliability	What is the Standard Operating Procedure (SOP) for denoting when an EVB return envelope is classified as a "No Signature?" The instructions on the EVB return envelopes are unequivocal: the voter MUST sign their name in the Signature Region; however, when there is a signature elsewhere, there are	pp. 64-67

	"VERIFIED AND APPROVED MCTEC" stamps on the envelopes. Disclosure of the SOP, or augmenting the SOP to define the rules of engagement in such instances may improve reliability in this process.	
Precision	The existence of 34,448 Duplicates: 2-copy, 3-copy, and 4-copy indicates opportunities for process improvements in ensuring that one voter gets only one EVB return envelope.	p. 62
Testability	One would assume that as the number of EVB return envelopes increases, there would be concomitantly more "Bad Signatures" i.e. Signature Mismatches. However, results indicate that the inverse took place in Maricopa in the general elections of 2016 and 2020. While the number of EVB return envelopes increased by 52%, the number of Signature Mismatches decreased by 59%.	pp. 29-31
Reproducibility	Only 587 – 0.031% of all EVB return envelopes – were identified by Maricopa election officials as "Bad Signatures." EchoMail classified 2,850 EVB return envelopes as having Scribbles. If EchoMail had been commissioned to perform Signature Verification, (which it had not), and deemed 2,850 Scribbles as "Bad Signatures" that would result in at least four times more "Bad Signatures" than reported by Maricopa. Given the Signature Verification process in Maricopa exceeded over 1.9 Million EVB return envelopes, 587 for "Bad Signatures" appears to be an exceedingly low number.	p. 29 pp. 67-68
Scalability	The receipt and processing of EVB return envelopes appear to have temporal periods of peaks and valleys. Sudden surges, for example, in certain classes of EVB return envelopes – such as Duplicates, Blanks and Scribbles – during the 11/04/2020 to 11/09/2020 have been observed. Are these observations systemic to the inability to handle large volumes during short periods or due to something else?	pp. 72-76
Robustness	The Signature Mismatch Rate in the State of Arizona for 2016 general election with EVB return envelopes of approximately 2 Million was 0.131%; however, in Maricopa County for the 2020 general	pp. 26-25 pp. 29-31 pp. 82-84

	election with approximately 1.9 Million EVB return envelopes, the Signature Mismatch Rate is 0.031%. Maricopa's 2020 Signature Mismatch Rate is 4 times less than the State of Arizona's Signature Mismatch Rate for 2016. Did new policies or legislation have an impact on this Signature Mismatch Rate reduction? Signatures vary immensely from highly legible to high illegible. There is a 27-point signature verification process in place in Maricopa to perform Signature Matching. Building confidence in Signature Matching can facilitate constituent confidence in Signature Verification process.	

Table 16: Systems properties ("ilities") that can be enhanced from the resolution of anomalies identified in this audit.

Table 16 has derived a set of engineering systems properties or "ilities": Transparency, Verifiability, Auditability (Chain of Custody), Reliability, Precision, Testability, Reproducibility, Scalability, and Robustness, that can advance the current EVB systems processes by addressing the anomalies detected in this audit. Enabling such advancement of election voting systems, however, demands both a culture where attention to detail, constant monitoring of anomalies – small or large, seemingly insignificant or monumental – is fostered, as well as nurturing leadership that inspires a systemic and pervasive attitude that welcomes feedback: positive or negative. The future efforts towards addressing these anomalies, therefore, provide a unique and historic opportunity for an engineering systems approach to advance the systems integrity of U.S. election processes.

EXHIBIT 22

Letter, Eugene A. DePasquale, Pennsylvania Auditor General, to Tom Wolf, Governor, Commonwealth of Pennsylvania (Dec. 13, 2019)

PERFORMANCE AUDIT REPORT

Pennsylvania Department of State

Statewide Uniform Registry of Electors

December 2019

Commonwealth of Pennsylvania
Department of the Auditor General

Eugene A. DePasquale • Auditor General

This page left blank intentionally

Commonwealth of Pennsylvania
Department of the Auditor General
Harrisburg, PA 17120-0018
Facebook: Pennsylvania Auditor General
Twitter: @PAAuditorGen
www.PaAuditor.gov

EUGENE A. DEPASQUALE
AUDITOR GENERAL

December 13, 2019

The Honorable Tom Wolf
Governor
Commonwealth of Pennsylvania
Room 225 Main Capitol Building
Harrisburg, PA 17120

Dear Governor Wolf:

This report contains the results of the Department of the Auditor General's (DAG) performance audit of the Statewide Uniform Registry of Electors (SURE) administered by the Department of State (DOS). This audit was conducted pursuant to the Interagency Agreement (agreement) entered into by and between DOS and DAG, effective May 15, 2018, and under the authority of Sections 402 and 403 of The Fiscal Code, 72 P.S. §§ 402 and 403.

This audit covered the period January 1, 2016 through April 16, 2019, unless otherwise noted, with updates through the report date, and focused on audit objectives, which were agreed upon and formalized in the agreement, as follows:

1. Assessment of whether records maintained within the SURE system are accurate and in accordance with the Help America Vote Act (HAVA) and Pennsylvania law.
2. Evaluation of the process for input and maintenance of voter registration records.
3. Review of security protocols of the SURE system.
4. Review of the efficiency and accuracy of the SURE system.
5. Review of the internal controls, methodology for internal audits and internal audits review process.
6. Review of the external controls, methodology for external audits and external audits review process.
7. Review of the methodology for the issuance of directives and guidance to the counties by DOS regarding voter registration and list maintenance.
8. Any other relevant information or recommendations related to the accuracy, operability, and efficiency of the SURE system, as determined by the Auditor General.

Further, this audit was conducted in accordance with applicable *Government Auditing Standards*, issued by the Comptroller General of the United States, except for certain applicable requirements that were not followed. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.[1] Significant scope limitations caused by a lack of cooperation and a failure to provide the necessary information by DOS, the Pennsylvania Department of Transportation (PennDOT), and four county election offices (counties), substantially impacted our ability to obtain sufficient appropriate evidence to fully achieve all audit objectives as described below and within *Finding 1*.

DOS' denial of access to critical documents and excessive redaction of documentation resulted in DAG being unable to fully achieve three of the eight audit objectives. Specifically, DAG was unable to accomplish the following: (1) Objective 1, the accuracy of the records maintained in SURE; (2) Objective 3, the review of security protocols of the SURE system; and (3) Objective 6, review of the external controls, methodology for external audits and external audits review process. This sustained refusal to cooperate with our information requests was done without DOS providing any plausible justification for their noncooperation. Accordingly, DAG was unable to establish with any degree of reasonable assurance that the SURE system is secure and that Pennsylvania voter registration records are complete, accurate, and in compliance with applicable laws, regulations, and related guidelines. See additional explanation in *Finding 1*.

As part of determining the accuracy of the voter registration records in SURE, we originally designed our tests to allow us to project the accuracy of the records over the entire population of 8,567,700 voters as of October 9, 2018 through the use of statistical sampling. We randomly selected 196 out of the 8,567,700 voters and requested source documents to verify the accuracy of the related voter data within SURE. While we found the records were accurate for the 58 voter records that we were able to test, we were unable to form any conclusions as to the accuracy of the entire population of voter records maintained in SURE since we could not test 138 or 70 percent of the records we sampled due to source documentation not being made available. The reasons that source documentation was not available for these records included DOS not providing adequate record retention requirements and guidance to the counties, counties not responding to our requests for source documentation, PennDOT's refusal to provide access to Motor Voter source documents, and DOS not maintaining online application source documents. Because of this, we could not conclude on our statistical sample and therefore, we could not project our results and ultimately conclude on the overall accuracy of the voter registration information maintained in the SURE system.

---

[1]U.S. Government Accountability Office. *Government Auditing Standards*. 2011 Revision. Please see the following summary of key standards: (1) Paragraphs 6.56 through 6.72 relate to standards related to obtaining sufficient appropriate evidence; (2) Paragraphs 6.23 through 6.27 relate to standards for evaluating the effectiveness of information system controls; and (3) Paragraph 6.36 relates to review of previous audits and attestation engagements.

Despite experiencing these difficult impediments throughout the audit, we were able to complete many audit procedures and believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. See *Findings 2 through 7* for our results. Overall, we provide 50 recommendations to strengthen DOS' policies, management controls, and the accuracy of the voter registration records in SURE, and to close gaps between leading IT security practices and the current policies, procedures, and practices protecting the SURE system. It is imperative for DOS to implement leading information technology security practices and information technology general controls to protect the SURE system and ensure the reliability of voter registration records. Additionally, it is imperative that DOS continue with its plans to develop and implement a replacement system to ensure the voter registration records are secure and accurate. DOS should also update current job aids and develop additional job aids and guidance to address issues such as duplicate voter records, records of potentially deceased voters on the voter rolls, pending applications, and records retention.

Based on data analysis that we were able to perform, despite the substantial scope limitations noted above, we identified tens of thousands of potential duplicate and inaccurate voter records, as well as voter records for nearly three thousand potentially deceased voters that had not been removed from SURE. We found that voter record information is inaccurate due to weaknesses in the voter registration application process and the maintenance of voter records in SURE. Specifically, voter registration applications remain in pending status for long periods of time- indefinitely in some cases, and although list maintenance activities are performed by counties, insufficient analysis and monitoring has resulted in inaccurate data in the voter records. Additionally, incorporating edit checks and other improvements into the design of the replacement system for SURE will reduce data errors and improve accuracy.

Finally, during the conduct of our procedures, we identified potential areas of improvement related to computer security, information technology general controls, and interface controls that we have specifically excluded from this report because of the sensitive nature of this information due to security concerns over the Commonwealth's critical elections infrastructure. These conditions and our recommendations have been included in a separate, confidential communication to DOS management.

We are very discouraged by management's response to our draft findings. We were quite surprised that DOS' response indicates that it strongly disagrees with many of our findings and mischaracterizes information that was provided, or not provided to us in many instances, during the course of our audit. With its attempt to refute our findings, DOS does not seem to understand that a primary objective of our audit was to assess the accuracy of records maintained in the SURE system. Our audit procedures disclosed internal control weaknesses related to input and maintenance of voter records, and our data analysis revealed examples of potential inaccuracies, all of which should be properly investigated by forwarding the information to the counties for further review. We are concerned that DOS, and therefore the counties, will not utilize the information provided to them in the audit because it is assuming that the data in the SURE system is accurate. Our data analysis strongly suggests otherwise. Also, while DOS requested

this audit, management does not seem to grasp that we cannot properly conclude and satisfy the audit objectives in accordance with generally accepted *Government Auditing Standards* without obtaining sufficient appropriate evidence, which they refused to provide to us.

In closing, despite the substantial limitations imposed by DOS, we believe we have provided DOS with recommendations that, if appropriately implemented, will improve the security of Pennsylvania's voter registration system and the completeness, accuracy, and auditability of its voter registration records. We hope that, despite its written disagreements, DOS seriously considers all of the management control weaknesses identified and works conscientiously with the counties to address all of the potential voter registration inaccuracies noted in the SURE voter registration records. We will follow up at the appropriate time to determine whether and to what extent all recommendations have been implemented.

Sincerely,

Eugene A. DePasquale
Auditor General

A Performance Audit

Pennsylvania Department of State
Statewide Uniform Registry of Electors

TABLE OF CONTENTS

Executive Summary 1

Introduction and Background 8

Finding One: **As a result of the Department of State's denial of access to critical documents and excessive redaction of documentation, the Department of the Auditor General was severely restricted from meeting its audit objectives in an audit which the Department of State itself had requested** 16

Recommendations 25

Finding Two: **Data analysis identified tens of thousands of potential duplicate and inaccurate voter records, as well as voter records for nearly three thousand potentially deceased voters that had not been removed from the SURE system** 27

Recommendations 36

Finding Three: **The Department of State must implement leading information technology security practices and information technology general controls to protect the SURE system and ensure the reliability of voter registration records** 38

Recommendations 43

Finding Four: **Voter record information is inaccurate due to weaknesses in the voter registration application process and the maintenance of voter records in the SURE system** 46

Recommendations 59

Finding Five: **Incorporating edit checks and other improvements into the design of the replacement system for SURE will reduce data errors and improve accuracy** 60

Recommendations 65

TABLE OF CONTENTS (continued)

Finding Six: **A combination of a lack of cooperation by certain county election offices and PennDOT, as well as source documents not being available for seventy percent of our test sample, resulted in our inability to form any conclusions as to the accuracy of the entire population of voter records maintained in the SURE system** 67

Recommendations 74

Finding Seven: **The Department of State should update current job aids and develop additional job aids and guidance to address issues such as duplicate voter records, records of potentially deceased voters on the voter rolls, pending applications, and records retention** 75

Recommendations 78

Agency's Response and Auditor's Conclusions 80

Appendix A – *Objectives, Scope, and Methodology* 134

Appendix B – *Interagency Agreement Between the Department of State and the Department of the Auditor General* 150

Appendix C – *Voter Registration Process* 157

Appendix D – *The lack of oversight that allowed non-citizens the ability to register to vote at PennDOT's photo license centers, even after indicating they are not a citizen, was addressed during the audit period* 161

Appendix E – *Voter Registration by County* 165

Appendix F – *HAVA Funds Received by Pennsylvania* 168

Appendix G – *Description of Data Used in the Audit* 172

Appendix H – *SURE Survey* 173

Appendix I – *Distribution List* 183

A Performance Audit

Pennsylvania Department of State
Statewide Uniform Registry of Electors

Executive Summary

This audit report presents the results of a performance audit of the Pennsylvania Department of State's (DOS) Statewide Uniform Registry of Electors (SURE). This audit was conducted pursuant to an Interagency Agreement (agreement) entered into by and between DOS and the Department of the Auditor General (DAG) on May 15, 2018.[2] The agreement specified eight audit objectives related to SURE and required the final report to be delivered by January 31, 2019. Additionally, the agreement specified that the audit time period would begin on January 1, 2016 and go through the end of our audit procedures.[3] Throughout the execution of this audit however, the auditors experienced scope limitations (addressed in *Finding 1* below) due to a lack of cooperation from DOS, the Pennsylvania Department of Transportation (PennDOT), and certain county election offices (counties), as well as a failure of those parties to provide DAG the necessary information needed to satisfy certain audit objectives. These delays resulted in the need to amend the agreement multiple times to extend the report release date as explained in *Appendix B*. In spite of these extensions, we were unable to fulfill all the requirements to conduct the audit in accordance with applicable *Government Auditing Standards* as described by the modified *Government Auditing Standards* compliance statement in the letter within this report and discussed further in *Finding 1*.

Despite these limitations, we believe that this report's seven findings and 50 recommendations as well as the comments and recommendations we have separately provided DOS within our confidential communication related to security protocols, information technology general controls, and interface controls will assist DOS, if appropriately implemented to improve the security of Pennsylvania's voter registration system and the completeness, accuracy, and auditability of its voter registration records.

Regrettably, we were surprised and disappointed that DOS' response contained in this report indicates that it strongly disagrees with many of our findings and mischaracterizes the information that was provided or not provided to us during the course of our audit. We address management's disagreements and mischaracterizations in the *Auditors' Conclusion* section of this report. We are concerned, however, with its attempt to refute our findings. DOS does not seem to understand that a primary objective of our audit was to assess the accuracy of records maintained in the SURE system. Our audit procedures disclosed internal control weaknesses related to input and maintenance of voter records, and our data analysis revealed examples of potential inaccuracies, all of which should be properly investigated by forwarding the information to the counties for further review. We are concerned that DOS, and therefore the counties, will not utilize the information provided to them in the audit because it is assuming that the data in the SURE system is accurate. Our data analysis strongly suggests otherwise. We hope that despite these written disagreements DOS seriously considers all of the management control

[2] See *Appendix B* for a copy of the agreement.
[3] Additional information on the audit scope, as well as the audit objectives and methodology can be found in *Appendix A*.

weaknesses identified and works conscientiously with the counties to address all of the potential voter registration inaccuracies noted in the SURE voter registration records prior to migrating this data into the new replacement system.

Our findings are summarized below.

Finding 1 – As a result of the Department of State's denial of access to critical documents and excessive redaction of documentation, the Department of the Auditor General was severely restricted from meeting its audit objectives in an audit which the Department of State itself had requested.

DOS failed to comply with the agreement's provision requiring that they cooperate with DAG's requests related to the audit. This failure impeded DAG's ability to timely conclude the audit and resulted in significant scope limitations that affected our ability to achieve audit objectives 1, 3, and 6. As a result, DAG was unable to determine with any degree of reasonable assurance that the SURE system is secure and that Pennsylvania voter registration records are complete, accurate, and in compliance with applicable laws, regulations, and related guidelines.

During the audit, DOS management denied us access to significant key documents/information related to the security and operation of the SURE system and for some documents that were provided, the entire documents were redacted, making the documentation unusable as evidence.[4] Without these critical documents, we were unable to satisfy our audit objective to review the security protocols of the SURE system (Objective 3). In addition, we were unable to comply with *Government Auditing Standards,* which require auditors to evaluate the effectiveness of IT controls and review previous audits and assessments significant within the context of our audit objectives. Without access to the external security assessment reports, we were unable to determine what information the assessments contained, and therefore, have no assurance that the assessments covered all of the various layers of security protecting the SURE system (Objective 6). We were also unable to determine if any security weaknesses were noted in the assessments or whether corrective actions had been implemented.

Additionally, due to the lack of cooperation from certain counties, PennDOT, and the system design of online voter registration applications, we were unable to perform adequate tests to determine the accuracy of the voter record data in SURE (Objective 1). We are, therefore, unable to form any conclusions as to the accuracy of the entire population of voter registration records maintained in SURE.

Despite experiencing these difficult impediments throughout the audit, we were able to complete many audit procedures, including some related to objectives 1, 3, and 6, and have discussed our

[4] After approximately nine months of requesting copies of certain reports, we were provided with hundreds, if not thousands of pages that were blacked out from top to bottom other than the report cover pages.

results in *Findings 2 through 7*. Within this finding, we offer six recommendations related to future audits of SURE or its replacement and the need for respective parties to cooperate with auditors.

Finding 2 – Data analysis identified tens of thousands of potential duplicate and inaccurate voter records, as well as voter records for nearly three thousand potentially deceased voters that had not been removed from the SURE system.

We requested SURE electronic files of all currently registered voters and the history of all of the changes made to voter records during the period January 1, 2016, to the present. We also requested copies of the Full Voter Export List for each county, which are available to the public through DOS' website. It took over three months for DOS to provide these electronic files. These files contained voter registration records for 8,567,700 registered voters as of October 9, 2018. Using these files, we performed data analysis to evaluate the information within SURE for reasonableness.

As a result of our data analysis, we identified potential inaccuracies, including:

- 24,408 cases where the same driver's license number was listed in more than one voter record.
- 13,913 potential duplicate cases.
- 6,876 potential date of birth (DOB) inaccuracies.
- 2,230 potential DOB and/or registration date inaccuracies.
- 2,991 records of potentially deceased voters.

Due to audit time constraints, we did not validate the thousands of cases/situations identified, and as a result, we use the term "potential" to be conservative. We believe, however, that in most of these instances, there are inaccuracies within the data maintained in SURE, and therefore, DOS will need to work with the counties to follow up and address all these situations in order to investigate and correct the voter records as appropriate.

Based on the results of our data analysis, along with reviewing DOS regulations and guidance, and on-site visits to seven counties where we observed staff processing new voter registration applications (applications) to check for duplicate records, we found the process ineffective for identifying duplicate records and removing voter records of deceased voters. We also identified other weaknesses increasing the risk of inaccurate records regarding the processing of applications and subsequent list maintenance, which are addressed separately in *Findings 4 and 5*.

We offer 10 recommendations to DOS to work with the counties to investigate these situations of potential duplicates, deceased voters, and inaccuracies and correct the voter records as appropriate; create automated processes to prevent duplicate and invalid information from being

recorded in the SURE system and/or the replacement system for SURE; and to evaluate the guidance provided to the counties regarding duplicates to ensure that it is adequate.

Finding 3 – The Department of State must implement leading information technology security practices and information technology general controls to protect the SURE system and ensure the reliability of voter registration records.

As described in *Finding 1,* DOS refused to provide us access to significant key documents related to the security, information technology (IT) controls, and operation of the SURE system. As a result, we were unable to satisfy our audit objective to review the security protocols of the SURE system and conduct our audit in accordance with applicable *Government Auditing Standards.*[5]

Based on the limited information that DOS management did provide to us or through review of other available information, we were able to identify gaps between leading IT security practices and the current policies, procedures, and practices protecting the SURE system and supporting architecture. We found that the governance structure of the SURE system and supporting architecture does not adequately define oversight and IT management in order to implement effective IT controls. Additionally, DOS management's vendor oversight practices need to be improved. DOS management could not provide System and Organization Control (SOC) reports for its key vendors or evidence that it reviewed the SOC reports and assessed whether controls at the service organizations were appropriately designed and operating effectively.

Further, we found that DOS management's county-level *SURE Equipment Use Policy* fails to provide clear guidance to counties for the appropriate use of the IT equipment provided by DOS. It also fails to include the additional responsibilities for security if the county chooses to connect county-owned equipment to the SURE system and a corresponding form to request and approve such deviation.

We offer one recommendation to the Secretary of the Commonwealth to consider creating an oversight body for the SURE system. We also offer 11 additional recommendations to DOS management to develop a governance structure that will provide clear lines of authority in the operation, maintenance, and security of the SURE system; continue with plans to replace the SURE system; implement additional security guidelines; monitor vendors through a documented process; and update the *SURE Equipment Use Policy*.

[5] U.S. Government Accountability Office. Government Auditing Standards. 2011 Revision.

Finding 4 – Voter record information is inaccurate due to weaknesses in the voter registration application process and the maintenance of voter records in the SURE system.

We found that the SURE system and supporting processes and controls are not effective to ensure that the voter registration information is accurate. We identified several reasons why inaccuracies occur and grouped them into two areas: (1) weaknesses within the application process, and (2) weaknesses regarding the maintenance of voter registration records within the SURE system.

Regarding weaknesses within the application processes, we found that no review is required to ensure that data on the application form is being accurately entered into SURE either at the time of data entry or on a routine basis after data entry. Automated edit checks and other features to prevent or detect inaccuracies are also not sufficiently incorporated into the SURE system. Additionally, we found that applications can remain in pending status for long time periods and in some cases indefinitely. Based on data analysis, as of October 9, 2018, there were 91,495 applications in pending status, including 23,206 that had been placed in pending status prior to the beginning of our audit period on January 1, 2016.

For weaknesses regarding the maintenance of voter registration records within the SURE system, we found that insufficient analysis by counties has resulted in inaccurate voter record data, despite the performance of list maintenance activities by the counties. Our analysis also identified 96,830 voters who potentially should be classified as inactive and an additional 65,533 records of inactive voters whose voter records potentially should have been canceled. Additionally, DOS does not fully utilize the list maintenance feature it pays for as a member of the Electronic Registration Information Center (ERIC).

We offer eight recommendations to improve application processing controls and the accuracy of the voter registration data.

Finding 5 – Incorporating edit checks and other improvements into the design of the replacement system for SURE will reduce data errors and improve accuracy.

In addition to the inadequate or nonexistent automated checks in the SURE system for allowing duplicate voter records, preventing adding a voter with a driver's license already associated with a voter record, and recording of obviously inaccurate birthdates and/or voter registration dates (addressed in *Finding 2*), we found features that were missing or inadequate which could further reduce or prevent errors. Specifically, we found that the SURE system does not prevent applications with a non-Pennsylvania residential address from being approved. The SURE system also lacks geographical mapping assistance which would reduce inefficiencies and potential inaccuracies by preventing applications from being sent to the wrong county for processing. Additionally, the SURE system lacks a "Read Only" feature to prevent key fields with permanent data such as a date of birth, Social Security number, or driver's license number

from being changed. Finally, the SURE system does not have controls in place to ensure that voter registrations are not improperly cancelled within 90 days of an election.

We were also informed of two additional areas needing improvement related to the PennDOT Motor Voter process and the reporting capabilities within the SURE system. We found that some individuals confuse the change of address prompt at PennDOT's photo license centers with registering to vote. Through discussions with DOS management and input from county officials, we also found that the ability to create reports in the SURE system is too limited and it lacks editable report capabilities.

We offer five recommendations to DOS that include incorporating several information technology enhancements into its design of the replacement SURE system and consider the feasibility of making some or all of these enhancements into the current SURE system. Additionally, DOS should consider working with PennDOT to revise the Motor Voter process to obtain all required voter registration information from individuals requesting to update their voter registration address.

Finding 6 – A combination of a lack of cooperation by certain county election offices and PennDOT, as well as source documents not being available for seventy percent of our test sample, resulted in our inability to form any conclusions as to the accuracy of the entire population of voter records maintained in the SURE system.

We selected a random statistical sample of 196 voters from the total population of 8,567,700 voters registered in SURE as of October 9, 2018. Our intent was to review source documents to confirm the accuracy of the information in SURE in the 196 voter records and thus conclude as to the accuracy of the entire voter population. Due to lack of cooperation and the unavailability of 138 of the 196 records selected (or 70 percent), we could not conclude on the accuracy of the entire voter population. Of the 196 voters selected, 84 of the voters' most recent application/change to their registration was made using a paper application. We were only able to test and verify the accuracy for 58 of these 84 paper applications. Of the remaining 26 applications, 14 could not be tested because 12 counties acknowledged that they were unable to locate the source documents needed to test each record for accuracy, and four counties did not respond to our requests to provide source documents for the other 12.

One factor for the unavailability of the applications is due to the lack of a clear records retention policy issued to the counties by DOS. Without clear guidance from DOS, we found that the counties have differing stances on how long an application must be kept. A clear record retention policy from DOS and a requirement to scan all applications into SURE would help ensure uniformity among counties, ensure complete records, provide a SURE user with the ability to answer questions if/when they arise from either voters or county staff, and allow for documents to be audited, as necessary.

We also found that DOS does not maintain copies, nor does it require the counties to maintain copies, of applications submitted via the online application process. This accounted for 19 of our 196 selected voters. Finally, for the remaining 93 applications processed through the Motor Voter system, PennDOT refused to provide us access to Motor Voter source documents.

We offer five recommendations to DOS to develop an audit trail for registration applications that are submitted online and via hard copy, develop a records retention policy to help ensure consistency of records retention amongst all the counties, and update the SURE regulations to ensure that they are in accordance with the newly developed records retention policy.

Finding 7 – The Department of State should update current job aids and develop additional job aids and guidance to address issues such as duplicate voter records, records of potentially deceased voters on the voter rolls, pending applications, and records retention.

We found that DOS generally provided meaningful assistance and guidance to the counties regarding SURE voter registration and list maintenance. DOS provides guidance to the counties related to the SURE system through job aids, which provide step-by-step instructions on how to complete various tasks associated with the processing of a voter registration application. Additionally, DOS also makes hands-on training available to the counties upon request. The counties and DOS also have access to the SURE Help Desk for assistance, as needed.

We believe, however, that the guidance provided by DOS did not sufficiently address all critical areas. The critical areas not adequately addressed include: job aids need to be updated to reflect recommended improvements regarding review for duplicate voter records and records of potentially deceased voters on the voter rolls, no guidance was provided to the counties regarding the length of time that applications remain in pending status and whether pending applications past that timeframe should be denied, and no clear guidance was provided to the counties regarding a record retention policy for voter record source documents. Additionally, we found that the job aids did not consistently contain uniform issue or revision dates in order to maintain version control and prevent confusion.

We offer four recommendations to DOS to continue to offer hands-on training on the SURE system; update the applicable job aids to reflect changes in processes; include an issue date on all job aids distributed to the counties and create an indexed list of job aids listing the most current version; and provide guidance to the counties regarding the maximum length of time that an application can remain in pending status.

Introduction and Background

This report presents the results of our performance audit of the Pennsylvania Department of State's (DOS) Statewide Uniform Registry of Electors (SURE). The performance audit was conducted under the authority of Sections 402 and 403 of The Fiscal Code and pursuant to the Interagency Agreement entered into by and between the Pennsylvania Department of the Auditor General and DOS.[6] Our performance audit had eight objectives and covered the period of January 1, 2016 through April 16, 2019, unless otherwise noted, with updates through the report date. Refer to *Appendix A* of this report for a detailed description of the audit objectives, scope, and methodology.

In the following sections we will discuss:

- Threats to Pennsylvania elections
- The election-related responsibilities of DOS and county election offices
- The implementation of SURE
- The Commonwealth's voter registration process
- The voter record maintenance process
- The status of Pennsylvania's voting systems
- DOS plans to replace the SURE system

Threats to Pennsylvania Elections

An accurate voter registration system and effective paper record voting machine system are critical in the current environment where a significant threat of hacking election records exists. In September 2017, the *New York Times* reported that earlier that month, the United States Department of Homeland Security had informed 21 states that their election systems had been ". . . targeted by hacking efforts possibly connected to Russia" during the 2016 Presidential election. The *New York Times* listed Pennsylvania as one of the states that informed the Associated Press that they had been targeted.[7]

In May 2018, the United States Senate Intelligence Committee (Intelligence Committee) released an unclassified summary of its investigation into the matter, confirming that cyber actors affiliated with the Russian government scanned state systems extensively throughout the 2016 election cycle. These cyber actors made numerous attempts to access several state election systems and, in a small number of cases, actually accessed voter registration databases. The

[6] 72 P.S. §§ 402 and 403. See *Appendix B* for a copy of the Interagency Agreement.
[7] <https://www.nytimes.com/2017/09/22/us/politics/us-tells-21-states-that-hackers-targeted-their-voting-systems.html> (accessed September 11, 2019).

investigation also found that at least 21 states potentially had their election systems targeted in some fashion while other states reported suspicious or malicious behavior.[8]

The targeting of state voter registration systems was confirmed by the Mueller Report, released in April 2019. This report found that officers of the Russian military intelligence agency used cyber hacking techniques during the 2016 presidential election to attack state boards of elections, secretaries of state, and county governments involved in the administration of elections, as well as individuals who worked for those entities.[9]

The Mueller report noted for example, that the Illinois state Board of Elections reported that hackers had succeeded in breaching its voter systems by sending malicious code to the state's website in order to run commands and gain access to the database containing the information for millions of registered voters.[10] The Mueller report also noted that Florida county election administration officials were targeted through spear-phishing emails that allowed the intruders to gain access to the network of at least one Florida county government.[11]

In July 2019, the Senate Select Committee on Intelligence reported that additional information was obtained in late 2018 that evidenced the U.S. election infrastructure of all 50 states, which includes voter registration databases, had been scanned by foreign agents in attempts to understand the networks and identify vulnerabilities within the systems at both state and local levels.[12] These events demonstrate the need for ensuring the security of Pennsylvania's voting systems against cybersecurity attacks which are increasing in both quantity and sophistication. Improving voting systems will simultaneously endeavor to maintain the utmost integrity in Pennsylvania election results.

The Election-Related Responsibilities of DOS and County Election Offices

DOS' Bureau of Election Security and Technology (BEST) oversees the functions of SURE, election security and technology initiatives, certification of equipment, and technology and data

[8] U.S. Senate Intelligence Committee, *Russian Targeting of Election Infrastructure during the 2016 Election: Summary of Initial Findings and Recommendations*, dated May 8, 2018. <https://www.intelligence.senate.gov/press/senate-intel-committee-releases-unclassified-1st-installment-russia-report-updated> (accessed February 27, 2019).
[9] U.S. Department of Justice, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, March 2019, page 50 <https://www.justice.gov/storage/report.pdf> (accessed April 22, 2019).
[10] Ibid.
[11] Id. at page 51.
[12] *Report of the Select Committee on Intelligence, United State Senate, on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, pages 3-12, <https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf> (accessed August 1, 2019).

innovation. BEST is also responsible for working with federal, state, and local partners to maintain and enhance the security of Pennsylvania's elections infrastructure.[13]
DOS' Bureau of Election Services and Notaries (BEN) oversees the functions of the Division of Election Services and Voter Registration. BEN is responsible for areas such as serving voters, candidates, counties, and other stakeholders on matters relating to election administration and voter registration.

DOS also oversees elections in conjunction with the county elections and/or voter registration office(s) in each of Pennsylvania's 67 counties. Staffing for these county election offices (county) range from 1 to 100 full-time employees, as well as some part-time/temporary employees as needed. County election/voter registration staff report to the County Commissioners/County Executive and are responsible for conducting elections and performing related tasks, including, but not limited to:

- Completing all tasks related to voter registration, including processing voter registration applications; performing procedures to update and monitor the accuracy of voter registration records, typically and hereafter referred to as *list maintenance*; and certifying voter registration statistics to DOS prior to each election
- Processing county level candidates' petitions for inclusion on the ballot
- Designing/printing the ballots
- Purchasing voting machines[14]
- Programming voting machines
- Printing poll books
- Hiring and organizing poll workers
- Finding/securing polling locations
- Certifying the election results to DOS

It is important to note that while DOS oversees Pennsylvania's elections and maintains the SURE system, the voter registration records are owned by the individual counties. If a voter moves from one county to another, any paper documents associated with that voter are transferred to the new county. DOS does not have ownership over the records, nor does it have the authority to edit records, cancel a record, or move a voter from active to inactive status.

The Implementation of SURE

The Help America Vote Act of 2002 (HAVA) was enacted to improve voting systems and voter access throughout the nation. HAVA created mandatory minimum standards related to key areas of election administration that every state must follow, one of which was to implement a

[13] For purposes of this report, we refer to BEST collectively as DOS.
[14] The counties have the authority and mandate to purchase voting machines; however, they may only purchase machines that have been certified by the federal government and by Pennsylvania's Secretary of State.

computerized statewide voter registration list to serve as the single system for storing and managing the official list of registered voters.[15] While DOS has had authority over elections in Pennsylvania since the early 1900s, it was charged with maintaining the SURE system shortly after HAVA's enactment.[16] SURE, which was implemented in Pennsylvania as a result of Act 3 of 2002, is the platform that supports the critical functions of the Commonwealth's election system, including voter registration, voter list maintenance, precinct data, and the production of poll books.[17] SURE was designed to ensure the accuracy and integrity of the Commonwealth's voter registration records maintained by the election authorities in each of the 67 counties.

SURE is maintained by DOS and utilized by each of the counties. DOS must ensure that the counties fulfill their statutory responsibilities, but DOS must be careful not to infringe upon functions reserved for the counties (as discussed above, the counties own the voter registration records, not DOS). For example, the counties have the authority to process voter registration applications, make changes to a voter's record, or cancel a voter's registration; however, HAVA requires DOS to ensure that the voter registration records are accurate and are updated regularly. This includes "file maintenance that makes a reasonable effort to remove registrants who are ineligible to vote."[18] Accordingly, HAVA places the responsibility on DOS to ensure that SURE data is accurate but at the same time, DOS has no ability to force the counties to comply.

The Commonwealth's Voter Registration Process

Any individual who wants to vote in an election in Pennsylvania is required to register to vote no later than 30 days prior to the election. The National Voter Registration Act (NVRA) requires that:

- Each State shall designate agencies for the registration of voters in elections for *Federal office*.
- Each State shall designate as voter registration agencies:
  - all offices in the State that provide public assistance
  - all offices in the State that provide State-funded programs primarily engaged in providing services to persons with disabilities.[19]

[15] 52 U.S.C. § 21083(a)(1).
[16] As part of the SURE system, DOS also created the SURE Portal (Portal). The Portal allows the user to view but not edit or cancel a voter's record. The Portal is used by county staff, especially during periods of high activity, and by the BEST staff to answer telephone calls from voters requesting their status (registered or not), their party affiliation, or the location of their polling place.
[17] 25 Pa.C.S. § 1222.
[18] 52 U.S.C. § 21083(a)(2).
[19] 52 U.S.C. § 20506(a). For the purposes of voter registration, as required by the NVRA, the offices in Pennsylvania that have been identified as those that "provide public assistance" are: Women, Infant and Children Nutrition Clinics; County Assistance Offices; Clerk of Orphans' Courts, Children and Youth Agencies; Area Agencies on Aging; Para-Transit providers; Special Education Programs at the 14 state-owned universities; agencies

Pennsylvania, through its voter registration law, has included these requirements for all elections.[20]

The ways in which a person can register, as well as the qualifications to register, are standardized throughout Pennsylvania and are outlined in *Appendix C*. The application to register is received and processed by the county. The SURE system guides the county staff through the process; however, the number of applications received varies greatly and the manner in which a county distributes work is discretionary within each county.

Anytime an individual submits a voter registration application (application) that is able to be processed, whether it is to initially register to vote or to change their name/address/party, the applicant will be mailed a voter card that contains the voter's information and the name and location of the corresponding polling place.[21] The voter card is mailed "non-forwardable" and if it is not returned to the county within 10 days, the applicant becomes a registered voter. Once an applicant is a registered voter, they are eligible to vote in the next election. If the voter is a new voter or voting for the first time at a polling place, the voter will need to show proof of identification (see *Appendix C* for a list of acceptable forms of identification). See *Appendix E* for information on 2018 Pennsylvania voter registration statistics.

The NVRA also requires that the Pennsylvania Department of Transportation (PennDOT) provide its customers an opportunity to register to vote.[22] Commonly referred to as "Motor Voter," this process provides PennDOT customers the ability to register to vote while applying for or renewing a driver's license or photo ID at a PennDOT center. Being fully electronic since 2003, any voter registration applications obtained by PennDOT are uploaded into SURE and are electronically distributed to the applicable counties for processing. A defect detected with the Motor Voter system, which permitted non-U.S. citizens to request to register to vote, is discussed in *Appendix D*. The following table shows the number of new voter registrations and change of address edits made to SURE voter records resulting from voters' usage of PennDOT's Motor Voter system during the calendar years 2015 through 2018:

---

serving people with disabilities and County Mental Health/Intellectual Disabilities offices; and the armed services recruitment centers.

[20] 25 Pa.C.S. § 1325.

[21] An application should not be processed if it is missing information or if it is an exact duplicate of the information for a voter already within the system.

[22] 52 U.S.C. § 20501 *et seq.* which is also known as the Motor Voter Act.

Pennsylvania Department of State Number of Voter Registration Transactions Processed Through PennDOT's Motor Voter System by Transaction Type for Calendar Years 2015-2018				
Type of Transaction	**2015**	**2016**	**2017**	**2018**
New Registration	112,774	112,680	94,946	98,911
In-County Change of Address	295,377	321,410	369,727	346,899
Out-of-County Change of Address	91,468	92,466	111,260	106,930
Total[a/]	**499,619**	**526,556**	**575,933**	**552,740**

[a/] The numbers reported only reflect transactions that were forwarded from PennDOT to DOS that resulted in a new registration or change made to an existing registration. Therefore, these numbers do not include applications that were unable to be approved/processed, such as those with incomplete information, applications for individuals that are already registered to vote, or for those individuals that were not eligible to register to vote.
Source: Produced by the Department of the Auditor General staff based on information from the Pennsylvania Department of State's "The Administration of Voter Registration in Pennsylvania, Report to the General Assembly" for calendar years 2015-2018, dated June 2016, June 2017, June 2018, and June 2019, respectively.

The Voter Record Maintenance Process

Voter registration data is continuously maintained by the individual counties through the SURE system. In addition to ongoing maintenance, the counties conduct annual maintenance activities as prescribed by law.[23] For instance, the counties send address verification notices to voters who have been identified by the United States Postal Service as having submitted a change of address. Counties send Five-Year Notices to voters who have not voted in the past five years or made any contact with the county. If the voter fails to respond to the mailing, they are marked as inactive. Once a voter is marked as inactive, the voter will remain in that status until they vote or update their information. An inactive voter can still cast a ballot at their polling location, but must sign an affidavit confirming their address. Once the affidavit is signed, the voter is able to vote and will be moved back to active status in SURE as part of a post-election process. If the voter fails to vote in the next two consecutive general elections for federal office (four or more years after being moved to inactive status), the county should cancel the voter's registration.

In addition to cancelling a voter's registration due to inactivity, a county should cancel a voter's registration if the county receives a written request from the voter to have their voter registration cancelled or is notified that the voter died or moved out of state. The following table summarizes the number of active and inactive voters whose registrations were cancelled and the reason for cancellation in the calendar years 2015-2018:

[23] 52 U.S.C. § 21083(a)(2) and 25 Pa.C.S. § 1901(b)(1)(i).

Pennsylvania Department of State Number of Active and Inactive Voters Cancelled by Reason for Calendar Years 2015-2018						
Calendar Year and Voter Status	**Cancelled at Voter's Request**	**Cancelled due to Voter's Death**	**County Confirmed Change of Address[a/]**	**PennDOT Confirmed Change of Address**	**Voter Removal Programs[b/]**	**Total**
2015 Active	1,280	91,951	20,405	86,476	5,955	206,067
2015 Inactive	351	13,321	5,713	10,473	156,107	185,965
2016 Active	1,605	76,987	100,956	90,565	3,935	274,048
2016 Inactive	374	11,799	23,328	11,253	83,515	130,269
2017 Active	1,859	93,649	21,963	101,984	3,979	223,434
2017 Inactive	251	10,264	3,761	8,018	233,517	255,811
2018 Active	2,311	79,178	50,602	95,332	3,458	230,881
2018 Inactive	516	12,246	12,019	10,916	113,576	149,273

[a/] Includes if the county visited the address on record to confirm the voter no longer lives there.
[b/] Cancelled because no response was received after various mailings.
Source: Produced by the Department of the Auditor General staff based on information from the Pennsylvania Department of State's "The Administration of Voter Registration in Pennsylvania, 2018 Report to the General Assembly" dated June 2019.

The Status of Pennsylvania's Voting Systems

HAVA not only requires that each state has a general registry for voter registration, it also placed mandates on the states regarding voting systems. While HAVA was a funded mandate (see *Appendix F* for federal money received by Pennsylvania, by year) from the federal government, the money has waned in the past several years. Technology however, continues to evolve, and the HAVA-compliant voting machines purchased over a decade ago are reaching or have already reached, the end of their useful life. In April 2018, DOS informed all counties that they must select a voter-verifiable, paper record voting system no later than December 2019, but ideally they should have one in place for the November 2019 election.[24] At the time of this mandate, the voting systems in use in 50 of the 67 counties in Pennsylvania did not have the ability to record votes with a hard-copy record and, therefore, were not in line with the new mandate from DOS. DOS received $14.15 million in August 2018.[25] This money has been used to assist the counties in replacing their voting systems, however, this amounts to only approximately 10 percent of the estimated total statewide cost of $150 million.[26] In October 2019, an election reform bill was

[24] <https://www.governor.pa.gov/governor-wolf-statement-directive-new-voting-machines-paper-record/> (accessed May 16, 2019).
[25] This $14.15 million consisted of 95 percent federal funding and a 5 percent state match.
[26] County Commissioners Association of Pennsylvania, *Election Equipment and Voting Systems*, <https://www.pacounties.org/GR/Documents/1-ElectionEquipmentPriorities2019.pdf> (accessed May 16, 2019).

signed into law by Governor Wolf that included $90 million to assist the counties with purchasing new voting systems.[27]

All voting systems to be used in Pennsylvania must be certified by both the federal Election Assistance Commission and the Secretary of the Commonwealth.[28] As of June 13, 2019, DOS (via the Secretary) certified seven new voting systems for use in Pennsylvania.[29]

DOS Plans to Replace the SURE System

As noted above, the SURE system in place today was initially implemented and rolled out beginning in 2003, making it over 15 years old. DOS management stated that they are starting the process to obtain and implement a new SURE system. DOS is currently working with the Office of Administration, Office for Information Technology to develop a request for proposal to replace the SURE system.

[27] *See* Act 77 of 2019, enacted October 31, 2019 (Immediately effective with exceptions).
[28] 25 P.S. § 3031.5.
[29] <https://www.media.pa.gov/Pages/State-Details.aspx?newsid=342> (accessed September 23, 2019).

Finding 1 – As a result of the Department of State's denial of access to critical documents and excessive redaction of documentation, the Department of the Auditor General was severely restricted from meeting its audit objectives in an audit which the Department of State itself had requested.

In November 2017, the Pennsylvania Senate's State Government Committee considered legislation that would require the Pennsylvania Department of the Auditor General (DAG) to audit the Pennsylvania Department of State's (DOS) Statewide Uniform Registry of Electors (SURE). Various members of our state legislature voiced concerns regarding the security of Pennsylvania's voting systems after several national media outlets reported allegations of foreign actors hacking multiple states' voter registration databases.[30]

DOS contacted DAG to discuss the pending legislation, and after various meetings between DAG, DOS, the Pennsylvania Governor's Office of Administration, Office for Information Technology (OA/OIT), and the Senate State Government Committee, it was agreed that DOS and DAG would enter into an Interagency Agreement (agreement) to conduct an audit which would accomplish the goals set forth in the proposed legislation. The agreement tasked DAG to audit the SURE system and outlined specific audit objectives to be performed that satisfied the interests of all parties involved.[31]

As the audit progressed, however, DOS failed to comply with the agreement's provision requiring that they cooperate with DAG's requests related to the audit. In addition to language in the agreement, Pennsylvania law requires DOS to cooperate with the DAG.[32] This failure impeded DAG's ability to timely conclude the audit and, as outlined in the table below, resulted in significant scope limitations that affected DAG's ability to achieve audit objectives 1, 3, and 6.

[30] More recently, there has been concerning news of hacking the databases of all 50 states and federal officials have noted major concerns about Pennsylvania's system. https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html and https://www.nytimes.com/2019/07/26/us/politics/states-voting-systems.html (accessed August 12, 2019).

[31] See *Appendix B* for a copy of the original agreement.

[32] Please note that Section 502 (relating to Cooperative duties) of the Administrative Code of 1929 provides as follows: "[w]henever, in this act, **power is vested in a department**, board, or commission, to inspect, examine, secure data or information, or to procure assistance, from any other department, board, or commission, **a duty** is hereby imposed upon the department, board, or commission, upon which demand is made, to render such power effective." (Emphasis added.) *See* 71 P.S. § 182 (Adm. Code § 502). This section of the Administrative Code clearly requires that whenever an administrative agency (DAG) has a power to secure an audit as provided in statute, any other agency (DOS or the Pennsylvania Department of Transportation) requested to provide such documents has the duty to be cooperative.

Objective Number	Objective	Able to Achieve Audit Objective	Detail Found in Finding Number
1	Assessment of whether records maintained within the SURE system are accurate and in accordance with the Help America Vote Act (HAVA) and Pennsylvania law.	No (See Scope Limitation B below)	2, 4, 5, 6
2	Evaluation of the process for input and maintenance of voter registration records.	Yes	4
3	Review of security protocols of the SURE system.	No (See Scope Limitation A below)	1, 3 [a/]
4	Review of the efficiency and accuracy of the SURE system.	Yes	5
5	Review of the internal controls, methodology for internal audits and internal audits review process.	Yes	4
6	Review of the external controls, methodology for external audits and external audits review process.	No (See Scope Limitation A below)	1 [a/]
7	Review of the methodology for the issuance of directives and guidance to the counties by DOS regarding voter registration and list maintenance.	Yes	7
8	Any other relevant information or recommendations related to the accuracy, operability, and efficiency of the SURE system, as determined by the Auditor General.	N/A[b/]	No Finding[b/]

[a/] - Due to its sensitive nature, we summarized the scope limitation in these findings, but included relevant detailed information in a separate confidential communication to DOS.
[b/] - While no other areas were added to the audit objectives and we do not have any findings or recommendations outside those related to the first seven objectives, see *Appendix D* regarding an issue that occurred during the audit period but was corrected prior to the beginning of the audit. The issue concerns the lack of oversight that allowed non-citizens the ability to register to vote at the Pennsylvania Department of Transportation's (PennDOT) photo license centers even after indicating they are not a citizen. We did not test for citizenship as part of this audit because citizenship information is not maintained in the SURE system, however, we did obtain from DOS certain information they were willing to provide regarding steps taken to address this issue. Other information regarding management's investigation and analysis of the situation was not provided. See further details in *Appendix D*.

After the agreement between DOS and DAG was executed on May 21, 2018, DAG promptly issued a standard engagement letter on May 22, 2018 to begin the audit. The engagement letter stated that DAG would release its final report on or before January 31, 2019, which was the date provided for in the agreement. Due to a lack of cooperation from DOS, PennDOT, and certain county election offices (counties), as well as a failure to provide the necessary information needed to satisfy the audit objectives, it became evident that DAG would not be able to perform the audit in accordance with certain applicable standards in *Government Auditing Standards*, which is issued by the U.S. Government Accountability Office. The standards in question included obtaining sufficient appropriate evidence, evaluating the design and operating

effectiveness of information technology (IT) controls, and reviewing previous audits and attestation engagements significant within the context of the audit objectives.[33] In February 2019, the original agreement was amended, and the date for final audit report release was extended to July 31, 2019. Due to a continued lack of cooperation from DOS in terms of providing requested information, this date was further postponed to September 27, 2019.[34]

The agreement included responsibilities of both DOS and DAG. The first responsibility listed for DOS was to **"cooperate with the Auditor General's requests involving the proposed audit"**; however, as discussed throughout the report, DOS did not provide us with responses to all of our requests. Instead of terminating the engagement due to lack of cooperation, which was justifiable under the terms of the agreement, in an effort to salvage an audit of paramount importance intended to enlighten Pennsylvania's electorate on the issue of election security and reliability, DAG issued a modified *Government Auditing Standards* compliance statement for this audit to account for the significant scope limitations that resulted from DOS' refusal to provide access to documentation and data required to complete the audit.

As a direct result of this sustained refusal to cooperate with our data requests without plausible justifications, DAG was unable to establish with any degree of reasonable assurance that the SURE system is secure and that Pennsylvania voter registration records are complete, accurate, and in compliance with applicable laws, regulations, and related guidelines. These weaknesses, despite the full performance of DAG under the terms of the agreement, combined with the recent increased threats from cyber intrusion, leaves serious questions and concerns regarding Pennsylvania's voter registration system and records.

The following sections describe in greater detail the various scope limitations, how each affected our abilities to satisfy the audit objectives, and the uncooperative nature of DOS, PennDOT, and certain counties throughout the audit.

[33] U.S. Government Accountability Office. *Government Auditing Standards*. 2011 Revision. Standards related to obtaining sufficient appropriate evidence are included in Paragraphs 6.56 through 6.72, standards related to evaluating the effectiveness of information system controls are included in Paragraphs 6.23 through 6.27, and standards related to review of previous audits and attestation engagements are included in Paragraph 6.36.
[34] Subsequently, DOS requested a further extension for the final audit report to be released by November 29, 2019.

DOS-Imposed Scope Limitations Impacting Audit Objective Achievement

Scope Limitation A

We attempted to document a complete understanding of the complex IT security landscape supporting the SURE system and evaluate the design and operating effectiveness of IT controls using a four-pronged approach:

1. Document the IT system landscape of the SURE system and its supporting infrastructure.

2. Document governance over cybersecurity using the National Institute of Standards and Technology Framework and review security assessments previously performed by outside entities.[35]

3. Document and test IT General Controls as defined by the US General Accountability Office, *Standards for Internal Controls in the Federal Government* (Green Book).[36]

4. Interview and survey county election offices and county IT staff.

During the audit, DOS management denied us access to significant key documents/information related to the security and operation of the SURE system and, for some documents that were provided, redacted information to the extent that the documentation was not usable as evidence. The following list identifies the key documents/information that were not provided (items 1, 2, and 5) or were heavily redacted (items 3 and 4):

1. Contents of external security assessment reports issued by the United States Department of Homeland Security (Homeland Security), as well as reports issued by private firms contracted to assess security.[37]

[35] The National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity,* consists of five steps: (1) Identify critical physical and software assets, threats, vulnerabilities, and risks; (2) Protect the system and infrastructure to ensure its security and resilience; (3) Detect the occurrence of a cybersecurity event in the system and infrastructure; (4) Respond to and contain a detected cybersecurity incident; and (5) Recover and restore system data, capabilities, and services impacted by a cybersecurity incident. See <https://www.nist.gov/cyberframework> (accessed June 11, 2019).

[36] We attempted to compare the policies, procedures, and practices over the SURE system to the IT General Control best practices described in Principle 11 of the S*tandards for Internal Controls in the Federal Government* (Green Book), issued September 2014. The Pennsylvania Governor's Office adopted these federal standards for all Commonwealth agencies within Management Directive 325.12, effective July 1, 2015.

[37] We confirmed with audit agencies in other states that their auditors are provided access to security assessment reports issued by private firms and at least one other state has received security assessment reports issued by Homeland Security.

2. Systems and Organization Control reports detailing the security practices in place at outside vendors key to the security and operation of the SURE system.[38]

3. Detailed information on system configuration and implementation of cybersecurity policies.

4. The formal results and corrective action plans from the 2018 test of the emergency recovery system.

5. Documentation of significant IT controls and system interfaces.

In lieu of these key documents, DOS instead provided us with an affidavit from the Chief Information Security Officer of the Employment, Banking, and Revenue Delivery Center of OA/OIT stating that IT security controls were in place. This affidavit however, does not provide sufficient, or even appropriate, audit evidence as a basis for conclusions.

Without these critical documents listed above, we were unable to satisfy our audit objective to review the security protocols of the SURE system (Objective 3). In addition, we were unable to comply with *Government Auditing Standards*, which requires auditors to evaluate the effectiveness of IT controls and review previous audits and assessments significant within the context of our audit objectives.[39] DOS's refusal to provide these documents resulted in our inability to provide a conclusion regarding the security of the SURE system. It is important to note that DOS originally requested this performance audit and agreed to the audit objectives, as well as for DAG to conduct the audit in accordance with *Government Auditing Standards*; therefore, its refusal to provide the documents is of great concern.

Additionally, as a result of not being provided access to the contents of the external security assessment reports, we were not able to determine what these assessments included and therefore, have no assurance that the assessments covered all of the various layers of security protecting the SURE system (Objective 6). We were also unable to determine if any security weaknesses were noted in the assessments or whether corrective actions have been implemented. Further, until our audit revealed that DOS had failed to enact a policy for marking, handling, sharing, and storing Election Infrastructure (EI) information, DOS was unaware of the vital importance of having such a policy.[40] This is deeply concerning because the absence of such a

[38] Systems and Organization Control (SOC) reports are reports on a service organization's controls by an independent auditor.
[39] U.S. Government Accountability Office. *Government Auditing Standards*. 2011 Revision. Paragraph 6.23 through 6.27.
[40] Department of State, *Policy on Election System Security Measures*, Version 1.1, issued April 23, 2019, which establishes DOS policy regarding the identification, marking, handling, storage, and protection of Election Infrastructure Information, was issued after our audit cutoff date of April 16, 2019 for information submissions so that the report could be prepared.

critical policy dealing with EI information is indicative of systems that lack adequate controls or uniformity of protocols.

It is also important to note that DOS had initially agreed to provide us with access to these security assessments on July 9, 2018, but on the very day that such reports were to be provided to DAG, DOS advised us that we were not permitted to view the reports due to "policy." We requested a copy of the DOS policy restricting access to these reports and were not provided the policy until late April 2019, over nine months later. The effective date of the policy that DOS eventually provided to us restricting access to these and other documents dealing with the SURE system was April 23, 2019, many months after we had been refused access to such records and many months after we had requested a copy of DOS' policy. If the security assessment reports were as sensitive as claimed by DOS, we are concerned that DOS had no policy in place dealing with such critical information until April of 2019.

Further, while DOS refused to permit DAG the ability to review these documents, in October 2018, we were provided with a list of **20** persons who had access to these reports. This list not only included one contractor who was not a Commonwealth employee, but it was unclear why the remaining **19** DOS and OA/OIT employees needed such access.[41] Finally, DOS repeatedly advised us that the security assessments were not to be provided because Homeland Security had designated election infrastructure as "critical infrastructure" which prevented DOS from releasing the reports to DAG. Despite repeated requests over six months for a statement in support of this contention, DOS claimed that they were unable to obtain such a statement from Homeland Security. During the course of our audit, we were able to determine that these types of reports are provided to auditors in another state and as noted below, Homeland Security did not have concerns about DOS sharing the reports with DAG.

In a letter dated August 17, 2018, DOS' Chief Counsel denied DAG's request to review the security assessment reports on the SURE system issued by Homeland Security and other outside entities citing that pursuant to the USA Patriot Act, Homeland Security designated election systems as part of critical infrastructure as defined under the Critical Infrastructure Information Act of 2002 (CIIA).[42] It was the opinion of DOS' Office of Chief Counsel that the outside security assessment reports were protected critical infrastructure information (PCII) and could only be accessed by those with an absolute "need to know" in order to perform homeland security duties.[43] The Auditor General traveled to Washington, D.C. to meet with representatives from Homeland Security who stated, however, that sharing the reports was left up to the discretion of each particular state.

---

[41] While the contractor is not an employee, he is a contractor who performs critical functions in the SURE system. While the contractor's duties are necessary for the operation and security of the SURE system, see *Finding 3* for our concerns about governance over the SURE system.
[42] *See* 42 U.S.C. § 5195c(e), 6 U.S.C. §§ 131-134, respectively.
[43] Yet, it was not clear whether all 19 DOS and OA/OIT employees actually needed access to the reports. Later in the audit, DOS represented that certain employees' access to these reports was revoked after our audit request made DOS question why the access had been granted.

We considered review of the security reports and access to sensitive security information to be so crucial to our audit objectives, that we offered to review the reports and sensitive information in a secure setting with DOS supervision. Our offers to provide these additional security measures were refused repeatedly by DOS. Without access to the reports we could not determine the following:

- If all of the servers and supporting infrastructure used in the SURE system were included in the security testing.
- If the external security assessors were provided unrestricted access and performed their work in accordance with standards.
- If all relevant controls were tested.
- If exceptions were noted.
- If appropriate corrective actions were implemented.

Without an independent assessment of these reports and any corrective actions taken by DOS in response to these reports, the public has no assurance that DOS is taking proper steps to secure the SURE system. We cannot, with any degree of certainty, have confidence in the security of the SURE system because we were not permitted to review the reports or the other documents/information we requested. Our offers to review reports and documents/information in strictly controlled settings make DOS' refusals to cooperate that much more difficult to defend.

Scope Limitation B

As part of our audit procedures, we selected a random, statistical sample of 196 voters from the total population of 8,567,700 voters registered as of October 9, 2018, with the intention of reviewing source documents to confirm the accuracy of the voter record information in SURE and to confirm that a signature was on file for the voters indicating that they had affirmed that they were legally qualified to vote (Objective 1).[44] Source documents include the voter registration applications or information provided by the individuals to update their voter record. Of the 196 voters in the sample, we were unable to verify the accuracy of information for 138 voters, or over 70 percent of the sample. Depending on the source of the voter's application, we found that:

- DOS maintained no source documentation for the 19 voter records reviewed that were created through online applications.

- PennDOT did not provide access to source documentation for the 93 voters who registered to vote through the Motor Voter process.

[44] Statistical sampling means to select a limited number of items from the population on a systematic or random basis, review/test those items, and then draw a conclusion about the entire population based on the results of the items selected for testing with a statistically measurable degree of confidence considering the accepted percent rate of tolerable error. Our statistical sample of 196 voters was determined based on a confidence level of 98 percent and a tolerable error rate of 2 percent.

- Four counties did not respond to our request for 12 paper applications.
- Twelve counties confirmed they did not have paper applications on file to support 14 paper applications.

Due to the lack of cooperation from certain counties, PennDOT (regarding information from the Motor Voter system), and the system design of online applications, we were unable to perform adequate tests to determine the accuracy of the voter record data in SURE. We are therefore unable to form any conclusions as to the accuracy of the entire population of voter registration records maintained in SURE. Inaccurate voter records could ultimately lead to ineligible individuals being able to vote in elections or one individual being able to vote multiple times. An accurate and effective voter registration system, as well as public confidence in such a system, is critical in the current environment where a significant threat of hacking election records and results exists. See *Findings 2 and 6* for further details.

Overall

The aforementioned scope limitations encountered during the audit contributed to our conclusion that the SURE data used in this audit has significant limitations.

The uncooperative nature of DOS, PennDOT, and certain counties throughout the audit.

Contributing further to the significant scope limitations, we found that DOS was not only uncooperative, which was inconsistent with our agreement and state law, it was untimely in providing us the information we needed in order to satisfy our audit objectives.[45] As quoted previously, the agreement required DOS to cooperate with DAG's requests related to this audit. Specifically, DAG's audit engagement letter stated that DOS shall provide us with requested information or documentation within three working days of the request, which is a standard business practice. It was further communicated to DOS that if this pre-established timeframe was insufficient and DOS would need additional time to prepare its response, DAG would approve a reasonable extension if requested.

We submitted 66 individual official requests for information to DOS throughout the audit. We received 11 responses within the pre-established three-day timeframe. The information for the other 55 however, was either never provided or not received by the due date and, with one exception, DOS never requested an extension. This equates to DOS being untimely for more than **83 percent of information requests** on the audit that they requested. Regarding items that DOS never provided, there were 11 such instances that information was not provided even after several months of our repeated attempts to obtain the information. Despite this unresponsiveness,

[45] *See* 71 P.S. § 182 (Adm. Code § 502).

we continued to send reminders to DOS regarding the outstanding requests for information and emphasized the importance of receiving the documentation requested. As seen in the following table, it took DOS weeks, or in some cases months, to respond to certain requests after numerous appeals from us.

DOS Delays in Responding to Audit Information Requests	
Length of Time that DOS was Late in Responding to Information Requests [a/]	**Number of Requests**
Never provided [b/]	11
61-94 days late	2
31-60 days late	7
15 – 30 days late	13
4 -14 days late	12
1-3 days late	10
Total	**55**

[a/] - Timeframes are based on calendar days.
[b/] - We received no information for nine requests and only received a portion of the information for two requests.

The information provided by DOS 94 days late was the voter registration records for the population of registered voters in SURE. DOS was aware that this information, which took over three months to provide, was absolutely critical to us for performing data analysis as part of our audit procedures. Additionally, as previously mentioned, PennDOT did not provide source documentation for the 93 voters in our sample that registered to vote through the Motor Voter process, and four counties did not respond to our request for 12 paper applications. Delays and uncooperativeness of this magnitude were not only inconsistent with our agreement and state law but had a detrimental effect on our ability to perform our audit procedures and satisfy the audit objectives.

As a result of repeated delays (several extending for many months), non-responses, and refusals to provide information responsive to our official requests, the agreed upon audit report release date had to be extended and DAG was forced to establish a cutoff date of April 16, 2019 for information submissions in order to ensure that sufficient time would be allotted to prepare the report.

Conclusion

Despite experiencing these difficult impediments throughout the audit, we were able to complete many audit procedures, including some related to audit objectives 1, 3 and 6, and report our results and recommendations in *Findings 2 through 7*, accordingly. Based on our interviews with DOS, OA/OIT, and county management executives; data analysis; on-site interviews and

observation of procedures at seven counties; written surveys of Pennsylvania's 67 counties; and other audit procedures as explained throughout our report; we report the following findings:

- Data analysis identified tens of thousands of potential duplicate and inaccurate voter records, as well as voter records for nearly three thousand potentially deceased voters that had not been removed from the SURE system. (see *Finding 2*)

- The Department of State must implement leading information technology security practices and information technology general controls to protect the SURE system and ensure the reliability of voter registration records. (see *Finding 3*)

- Voter record information is inaccurate due to weaknesses in the voter registration application process and the maintenance of voter records in the SURE system. (see *Finding 4*)

- Incorporating edit checks and other improvements into the design of the replacement system for SURE will reduce data errors and improve accuracy. (see *Finding 5*)

- A combination of a lack of cooperation by certain county election offices and PennDOT, as well as source documents not being available for seventy percent of our test sample, resulted in our inability to form any conclusions as to the accuracy of the entire population of voter records maintained in the SURE system. (see *Finding 6*)

- The Department of State should update current job aids and develop additional job aids and guidance to address issues such as duplicate voter records, records of potentially deceased voters on the voter rolls, pending applications, and records retention. (see *Finding 7*)

We believe that it is imperative that DOS management take steps to implement the recommendations that we were able to include in this report, albeit based on DAG's significantly restricted ability to perform standard auditing practices, to ensure the completeness, accuracy, and auditability of the voter registration data recorded in the SURE system.

Recommendations for Finding 1

We recommend for future audits that DOS:

1. Arrange for independent audits of all parts of the SURE system, supporting architecture, and connected systems using a comprehensive framework of security standards, which includes tests of IT general controls, tests of cybersecurity controls, vulnerability

assessments, and penetration testing. These audits should be performed annually and build on security assessments already performed.

2. Cooperate with auditors by providing them with full, confidential access to all information and documents, to comply with state law and to allow the auditors to satisfy the audit objectives, especially when requesting a particular audit to be performed by a fellow public agency charged with doing audits.

3. Provide appropriate and sufficient supporting evidence to back up its assertions that disclosure of certain materials to an auditing agency is legally impossible.

4. Encourage counties, PennDOT, and other related agencies involved in voter registration to cooperate with future audits.

5. Provide specific policies and direction from federal authorities supporting DOS' position in the event that it believes that it cannot provide information pursuant to security concerns.

6. Provide the results of audits recommended above to those charged with governance of the SURE system.

Finding 2 – Data analysis identified tens of thousands of potential duplicate and inaccurate voter records, as well as voter records for nearly three thousand potentially deceased voters that had not been removed from the SURE system.

As part of audit procedures to address the accuracy of the voter registration information contained in the Statewide Uniform Registry of Electors (SURE), on July 10, 2018 we requested electronic files of all currently registered voters and the history of all of the changes made to voter records, such as changes to a voter's name or address that were recorded during the period January 1, 2016 through present. We also requested copies of each county's Pennsylvania Full Voter Export List from the SURE system available to the public through the Department of State (DOS) website.[46] It took three months for DOS to provide the electronic files. The files contained voter registration records for 8,567,700 registered voters as of October 9, 2018.[47]

Using these files we performed the following:

- Selected a statistical sample of voter records to determine whether the information contained in SURE agreed with the information contained on the voter registration application (application). (see *Finding 6* for results and conclusions)

- Data analysis to evaluate the information within SURE for reasonableness. (see below)

Data Analysis[48]

To perform data analysis, we utilized software that allowed us to sort, classify, match, and validate information (data fields) within SURE to look for potential errors or inaccuracies within the fields.[49] Once identified, in certain instances, we also attempted through data analysis to

[46] As provided by 25 Pa.C.S. § 1404(b)(1) (relating to Public Information Lists), as well as the SURE Regulations at 4 Pa. Code § 184.14(b) (relating to Public Information Lists), DOS will provide the Full Voter Export List to requestors. This version of the Public Information List is a full export of all voters in the county and contains the following fields: voter ID number, name, sex, date of birth, date registered, status (e.g., active or inactive), date status last changed, party, residential address, mailing address, polling place, date last voted, all districts in which the voter votes (e.g., congressional, legislative, school district, etc.), voter history, and date the voter's record was last changed.

[47] See *Finding 1* for discussion regarding delays by DOS and scope limitations to the audit.

[48] In spite of the limitations with regard to completeness and accuracy of the information in SURE (See *Findings 1, 2, and 6*), we conducted additional data analysis and found that the voter table agreed with published reports and that the overwhelming majority of records in SURE were consistent throughout the various tables within the system. As a result, this data is considered reliable with significant limitations. See *Appendix A* for more information.

[49] The software we used included Excel and ACL. ACL data analytics is a data extraction and analysis software used for audit, fraud detection, and risk management. By sampling large data sets, ACL data analytics software is used to find irregularities or patterns in data records that could indicate control weaknesses or fraud.

assess the possible causes for the errors or inaccuracies. Weaknesses in the controls with regard to processing applications and subsequent list maintenance are separately addressed in *Finding 4.*

The following summarizes the results of our data analysis:

- **24,408 cases** – The same driver's license (DL) number listed in more than one voter record:
    - **18,536 potential duplicate cases** – A voter may have two or more records.
    - **5,872 potential cases** – Two or more voter records have the same DL number.
- **13,913 potential duplicate cases** – The same first name, last name, and date of birth (DOB) and/or last four digits of Social Security number (SSN) are shared by more than one voter record.
- **6,876 potential DOB inaccuracies** – The DOBs equate to voters being 100 years of age or older.
- **2,230 potential DOB and/or registration date inaccuracies** – The DOBs listed are after the registration date.
- **2,991 records of potentially deceased voters** – The same first name, last name, and DOB and/or last four digits of SSN match the Pennsylvania Department of Health (DOH) deceased files.

Throughout the remainder of this finding, we describe the results of our data analysis. Due to audit time constraints, we did not validate the thousands of cases/situations identified, and as a result, we use the term "potential" to be conservative. We believe, however, that in most of these instances, there are inaccuracies within the data maintained in SURE, and therefore, DOS will need to work with the counties to follow up and address all these situations in order to investigate and correct the voter records as appropriate.

24,408 Cases – The same DL number listed in more than one voter record.

Of the approximately 8.6 million voter records, 7,938,806 records contained DL numbers, which should be unique to only one person.[50] We analyzed data to determine if the same DL number appeared in more than one voter record and found 24,408 cases as noted below:

[50] A DL number is not required to register to vote.

Voter Registration Records with the Same DL Numbers as of October 9, 2018		
Number of Cases the Same DL Number is Listed in More than One Record[a/]	**Total Number of Records Involved**	**Personal Elements**
7,540	15,100	Same DL Number, First Name, and Last Name
10,329	20,715	Same DL Number and First Name only
667	1,336	Same DL Number and Last Name only
18,536	**37,151**	**Total Number of Potential Duplicate Cases**
5,872	11,768	Same DL Number, Different First and Last Name
24,408	**48,919**	**Total Records with Duplicate DL Number**

[a/] 24,305, or over 99 percent, of the total cases with potential duplicate records, were pairs of records. The remaining 103 instances consisted of three records containing the same DL number.

Source: This table was compiled by the staff of the Department of the Auditor General from data received from the SURE system. We determined that the reliability of this data had significant limitations in regards to completeness and accuracy as noted in Appendix A. Although this determination may affect the precision of the numbers we present, there is sufficient evidence in total to support our findings and conclusions.

As shown in the table above, we evaluated the information based on what personal elements were the same and summarized accordingly. More than 18,500 cases were found where the two records that matched the same DL number also matched either the first name, last name, or both. We consider these cases to be voters that potentially have two or more records within SURE (potential duplicate records). We will discuss the possible reasons that this occurred in the next section of this finding. Having two or more records could potentially allow a voter to vote more than once in an election.[51]

We also identified in the above table 5,872 cases, involving 11,768 records that had the same DL numbers but different first and last names. Although it is possible that a few of these cases relate to the same individual with more than one voter record, it is much more likely that these results indicate that a typographical error occurred when the DL number was entered into SURE. See *Finding 4* for weaknesses related to data entry errors and *Finding 5* for lack of edit checks.

13,913 Potential Duplicate Cases – The same first name, last name, and DOB and/or last four digits of SSN are shared by more than one voter record.

In addition to our analysis of DL numbers, we analyzed the remaining 8,518,781 records in SURE that either had no DL number recorded or had a unique DL number recorded and were not reported as duplicates above. We identified an additional 13,913 cases where two or more

[51] Voting more than once in an election is against the law and considered a felony offense of the third degree. *See* 25 P.S. § 3535 (relating to Repeat voting at elections).

records shared first name, last name, and one or more other personal elements as summarized in the following table:

Voter Registration Records with Other Duplicated Information as of October 9, 2018		
Number of Cases with Three or More of the Same Personal Elements[a/]	**Total Number of Records Involved**	**Personal Elements**
6,427	12,872	Same First and Last Name and DOB
7,230	14,506	Same First and Last Name and last 4 digits of SSN
256	525	Same First and Last Name, DOB, and last 4 digits of SSN
13,913	**27,903**	**Total records with other duplicated information**

[a/] - The vast majority of these cases were instances where a pair of records shared the same information; however, 68 cases (213 records in total) had three or more instances of duplicate information with up to 10 records sharing identical information for one voter. Of the 68 duplicates, 1 individual had 10 active records matching on first and last name, DOB, and last 4 digits of their SSN, while another individual had 5 active records matching on the same personal elements. The remaining 66 cases (198 records in total) consisted of sets of 3 potentially duplicate records.

Source: This table was compiled by the staff of the Department of the Auditor General from data received from the SURE system. We determined that the reliability of this data had significant limitations in regards to completeness and accuracy as noted in Appendix A. Although this determination may affect the precision of the numbers we present, there is sufficient evidence in total to support our findings and conclusions.

Because these 13,913 cases share three or more personal elements, we consider these as potential duplicate records (i.e., an individual potentially has more than one voter record). Again, it is incumbent upon DOS to work with the counties to evaluate these potential duplicate records to determine if in fact they are duplicate records or whether some of the personal elements may have been incorrectly entered into SURE. Having two or more records could potentially allow a voter to vote more than once in an election.

Ineffective process for identifying duplicate records.

One of the steps to process an application includes making sure that the individual applying to register to vote does not already have a voter record in SURE (i.e., to avoid creating a duplicate record). DOS regulations require, at a minimum, a duplicate check using the registrant's first and last name as well as DOB.[52] If upon examining those initial criteria county staff believes that the record may be a duplicate, the regulation indicates that staff then should use other criteria to assess duplication, including:

[52] 4 Pa. Code § 183.6. (relating to Uniform procedures for the commissions relating to the process for identifying and removing duplicate records in the SURE system).

- The unique identifier.[53]
- The last four digits of a registrant's SSN.
- The DL number of the registrant.
- The signature of the registrant.[54]

To ensure compliance with the regulations, DOS creates and distributes job aids that provide step-by-step instructions on how to perform the duplicate checks. Specifically, county staff are instructed to perform two duplicate checks: (1) same last name and same DOB; and (2) same first and last name. The job aid then notes that additional duplicate checks "*can be made*" and provides instructions on how to perform those additional duplicate checks, including checks for duplicate DL numbers.

In order to understand the duplicate check process, during our on-site visits to seven counties, we observed staff processing new applications check for duplicate records. We noted that when staff entered the voter information into SURE, several records associated with a particular name might be displayed. It is then up to staff to manually determine whether the application is a duplicate of a voter record already in SURE. Once county staff determine that the applicant does not have a duplicate record, they indicate that in SURE and continue processing.

Although this process appears to be in compliance with the respective job aids and the regulations, it is not effective in ensuring that duplicate records are not being created. The SURE system does not require staff to check for duplicate DL numbers, if available, which is a unique number to an individual and should be a key element for determining whether an individual already has a voter record. Additionally, as noted in the next section, using DOB as key criteria for identifying a unique person will not work if the DOB is not correct in SURE. Further, as noted previously, this process is generally a manual one and can be labor intensive. According to county staff, during certain times of the year, such as prior to the general election, the number of applications counties receive for processing becomes voluminous. Processing a lot of applications within a short period of time, however, can lead to errors and reduce the effectiveness of the process for identifying duplicates. We also noted that the SURE system does not have any automated edit checks or a "hard stop" that prevents staff from adding a voter registration record with a DL number that is already associated with an existing voter record.

Therefore, DOS needs to re-evaluate its regulations and job aids to develop a more effective duplicate check process, especially since DOS is looking into replacing the existing SURE system (see the *Introduction and Background* section) so that the replacement system for SURE is designed to prevent or detect and correct duplicate voter records.

[53] The unique identification number consists of a nine digit number plus a two digit county identifier. The nine digit number should stay with the voter if they move to a new county, but the two digit county identifier should be updated to reflect the new county of residence.
[54] 4 Pa. Code § 183.6.

6,876 potential DOB inaccuracies – The DOBs equate to voters being 100 years of age or older.

In addition to analyzing records for potential duplicate records, we conducted data analysis regarding the reasonableness of voters' DOB. DOS informed us that inaccuracies existed regarding DOBs due to DOBs not being a required field for registering to vote at some point prior to the Help America Vote Act of 2002 (HAVA). According to both DOS and county staff, when data was migrated into the SURE system from the 67 counties' systems, a "generic" DOB was entered for voters who did not have a DOB listed.

As part of our DOB reasonableness analysis, using the 8.6 million registered voters' files, we evaluated DOBs for voters whose SURE record indicated that the voter was 100 years of age or older. The following table provides a summary of the analysis:

Voter Registration Records Indicating that the Voter was 100 Years of Age or Older as of October 9, 2018		
Number of Registered Voters	**Number of Potentially Deceased[a/]**	**Age Range**
1,800	0	110 years of age or older – DOB recorded as January 1, 1800, January 1, 1900, or January 1, 1901
518	2	110 years of age or older – Other DOB recorded
4,558	134	100 through 109 years of age
6,876	**136**	**Total records indicating voter was 100 years of age or older as of October 9, 2018**

[a/] Of the 6,876 registered voters with DOB in the SURE system indicating that they were 100 years of age or older, 136 were also identified as potentially deceased (discussed later in the finding).

Source: This table was compiled by the staff of the Department of the Auditor General from data received from the SURE system. We determined that the reliability of this data had significant limitations regarding completeness and accuracy as noted in Appendix A. Although this determination may affect the precision of the numbers we present, there is sufficient evidence in total to support our findings and conclusions.

As noted in the table above, we identified three "generic" dates (January 1, 1800, January 1, 1900, and January 1, 1901) accounting for 1,800 of the 6,876 voters (26 percent) who are potentially 100 years of age or older. As these dates are not accurate DOBs, DOS needs to work with the counties to correct these inaccuracies as well as determine whether the voters are potentially deceased (see next section).

It is also unlikely that most of the 518 records with DOBs indicating the voters are 110 years of age or older are accurate. According to the most recent United States Census Report for 2010

(census report), the number of persons 110 years old and over was just 330 nationwide.[55] Similarly, many of the 4,558 records in SURE where the DOB indicates that the voter was between 100 and 109 years old are potentially inaccurate. According to the census report there were only 2,510 Pennsylvanians over the age of 100 in 2010.[56] Therefore, our analysis demonstrates the need to research these voters' records and correct these records, if necessary.

Without accurate DOBs in SURE, county staff may fail to detect duplicate records as discussed in the prior section. Additionally, it can prevent county staff from accurately matching DOH death files with SURE records potentially allowing deceased individuals to remain on the voter rolls (see last section of this finding for more information).

2,230 Potential DOB and/or Registration Date Inaccuracies – The DOBs listed are after the registration dates.

In addition to looking at the potential age of the voter, we also compared the DOB to the registration date for reasonableness. Since an individual cannot be born after registering to vote, this comparison would indicate that the DOB or the registration date would be inaccurate, although it is also possible that both could be inaccurate. We found 2,230 voter records in which the DOB listed is after the registration date.[57]

Of the 2,230 voter records that listed DOB after the registration date, we found through data analysis that the DOB in 1,943 records, or 87 percent, was changed on the same day: December 13, 2008. Given the voter registration date was prior to the DOB, these records were changed inappropriately at that time. We also noted that some of the voter registration dates in this group were listed as prior to the year 1900, obviously errors or additional cases where staff filled in a value to facilitate the transfer of records to the SURE system. Again, DOS will need to work with the counties in order to fix the inaccuracies found.

Weaknesses and concerns regarding DOBs.

As noted in this section and the previous section, there are several thousand potential inaccurate DOBs and probably thousands that we have not detected. In order for the information to be accurate in SURE, sufficient controls must be developed to reduce the likelihood of data entry errors. *Finding 4* describes the weaknesses identified during the audit regarding data entry errors. Additionally, *Finding 5* describes the need for the SURE system or its replacement system to

[55] US Census Bureau, Centenarians: 2010, 2010 Census Special Reports, December 2012, <https://www.census.gov/prod/cen2010/reports/c2010sr-03.pdf> (accessed April 8, 2019). As noted in *Appendix A*, data from the US Census Bureau is of undetermined reliability; however, this is the best data available. Although this determination may affect the precision of the numbers we present, there is sufficient evidence in total to support our findings and conclusions.
[56] Ibid.
[57] Two of the 2,230 records were also included in the table of voters 100 years old and over.

have a "read only" feature for certain personal elements that would not typically change, such as DOB. Further, DOS should consider developing an automated process that would prevent SURE and/or its replacement system from accepting obviously inaccurate DOBs as well as questioning dates that do not make sense, such as DOB after the registration date. These types of edit checks would help reduce data entry errors.

2,991 Records of Potentially Deceased Voters – The same first name, last name, and DOB and/or last four digits of SSN match DOH death files.

DOS has developed a process through the SURE system to provide the counties with death records from DOH to help the counties identify and cancel deceased voters' records. According to instructions in the job aid (described in detail in *Finding 7*) related to processing death records, for each individual included in the death record, county staff should do a search in SURE for voter records that match on the last name and DOB. A second search is then done based on first and last name (in essence, the same process as searching for duplicate records for a new application previously discussed). County staff then manually compares the death record information to the list of voter records that were matches in the two searches performed to determine if the deceased individual has a voter record. Staff can perform additional searches of voter records to include information such as an address to assist in determining if a voter record is a match. If county staff determines that a voter's information matches a deceased individual in the death record, they are to cancel the voter's record in SURE.

To determine whether there were voter records within SURE that should have been cancelled due to deaths, we first independently requested and obtained from DOH death files from the period October 1, 2010 through October 9, 2018. [58] Next, using data analysis, we compared those files to the SURE records as of October 9, 2018, and grouped the matches based on the number of personal elements that agreed and the time period that the individual was deceased per DOH records, as shown in the below table:

[58] These data were supplied by the Bureau of Health Statistics & Registries, Pennsylvania Department of Health. The Pennsylvania Department of Heath specifically disclaims responsibility for any analyses, interpretations, or conclusions.

Analysis of Potentially Deceased Individuals as of October 9, 2018				
Number of Voters Matching Four Elements[a/]	**Number of Additional Voters Matching Three Elements[b/]**	**Total Number of Voters[c/]**	**Percentage of Total**	**Time as Registered Voter After Date of Death (As of October 9, 2018)[c/]**
131	158	289	10%	181 days to 1 year
550	489	1,039	35%	Over 1 year up to 3 years
501	440	941	31%	Over 3 years up to 5 years
391	331	722	24%	Over 5 years
1,573	**1,418**	**2,991**	**100%**	**Total**

[a/] - Includes those voter records that matched first name, last name, DOB, and last four digits of SSN.
[b/] - Includes those voter records that matched using two different sets of matching elements: first name, last name, and last 4 digits of SSN; first name, last name, and DOB.
[c/] - Due to timing and to be conservative, we did not include 1,258 voters who matched three or four elements whose date of death occurred less than 181 days prior to October 9, 2018.

Source: This table was compiled by the staff of the Department of the Auditor General from data received from the SURE system and from data received from DOH. As noted in Appendix A, we determined that the reliability of the SURE data had significant limitations in regards to completeness and accuracy and that DOH death data was data of undetermined reliability. Although this determination may affect the precision of the numbers we present, there is sufficient evidence in total to support our findings and conclusions.

Based on the above results using the independent data files we received from DOH, we conducted further data analysis to verify that DOH information was in fact received by DOS for the 2,991 potentially deceased voters. Our data analysis found that DOS had received at least 2,094 of the 2,991 death notices by DOH, but the record had not been cancelled as of October 9, 2018. This appears to indicate that counties received the death notice information for at least 2,094, but determined the result to not be a match. As previously stated, this is a manual process that depends on the accuracy of the data in SURE and the judgment of the county staff performing the review. If staff are reviewing the file too quickly or a piece of personal information is inaccurately listed in the voter record (such as previously described inaccurate DOBs) and therefore does not match, they may incorrectly dismiss the deceased individual record as not being a match.

Additionally, the 897 potentially deceased voters that did not seem to have a death notice could have been caused by our data analysis procedures failing to identify the SURE DOH application record because of misspellings in SURE and/or DOH death files. On the other hand, it could also indicate that there may be a problem in how DOH death files are transmitted to DOS. The process to provide DOS, and subsequently the counties, with death records is designed so that the counties only receive new death records. This is done to avoid counties having to review duplicate records. If, however, there is an update to the record of a deceased individual, this update may not be forwarded to DOS and subsequently the counties. As a result, a deceased

voter's registration may not be cancelled.[59] It is important that DOS investigate with DOH to determine if all appropriate death information is being provided to DOS so all appropriate, updated, and corrected death information is provided to the counties for processing. Failure to timely remove a deceased voter record increases the risk that records maintained within the SURE system are not accurate and therefore, not in compliance with HAVA.

Recommendations for Finding 2

We recommend that DOS:

1. Evaluate the lists of voter registration records with the same DL numbers and potential duplicate cases provided by DAG and work with the county election offices to investigate and eliminate the specific duplicate information identified during the audit.

2. Perform additional data analysis and cleansing procedures and work with the counties to remove duplicate and incorrect data from the SURE system before migration into the replacement system for SURE.

3. Create automated processes, such as a "hard stop," to prevent the inclusion of duplicate DL numbers in the design of the replacement system for SURE.

4. Evaluate and update, as needed, the instructions provided to the counties in the SURE job aids to ensure they provide adequate guidance on how to check for duplicates in the SURE system or the replacement system for SURE.

5. After conducting the cleansing procedures outlined in Recommendation 2 in preparation for migrating to the replacement system for SURE, perform periodic data analysis to ensure that duplicate records created in error are identified and removed from SURE in a timely manner.

6. Evaluate the lists of voter records provided by DAG with a DOB listed in SURE as January 1, 1800, January 1, 1900, or January 1, 1901 and who appear to be 100 years of age or older and instruct the counties to determine the correct DOB and ensure the record is still valid and the voter is not deceased.

[59] For example, if the original death record that was sent to DOS and subsequently to a county had an incorrect birthdate listed, then the county probably would not have cancelled the voter's registration due to the non-match of the birthdate. If the birthdate was later corrected to update the DOH record, this update may not be forwarded to DOS because DOH would recognize the deceased name as one that was previously sent to DOS. The county, therefore, would not receive the updated record with the correct birthdate that would provide the match and prompt the county to cancel the deceased voter's registration.

7. Create automated processes in the replacement system for SURE to prevent the recording of obviously inaccurate DOBs and voter registration dates (e.g., voter registration dates prior to DOB).

8. Evaluate the lists of potentially deceased voters provided by DAG and instruct the counties to investigate and take appropriate action to cancel deceased voters' records in SURE.

9. Consider an additional periodic comparison of the cumulative file of deaths received from DOH to records in SURE to identify any voters that may have been missed during past reviews. DOS should consider performing the match using data analysis techniques and provide matching records to the counties for follow-up.

10. Work with DOH to ensure the process is working properly regarding forwarding death records to DOS with all relevant, appropriate, and corrected information so that counties can evaluate the information and cancel the voter registrations of deceased individuals.

Finding 3 – The Department of State must implement leading information technology security practices and information technology general controls to protect the SURE system and ensure the reliability of voter registration records.

The Statewide Uniform Registry of Electors (SURE) was established, in part, to ensure the integrity and accuracy of all registration records in the system by prohibiting unauthorized entry, modification, or deletion of registration records.[60] Protecting the SURE system to ensure the reliability of voter registrations is of utmost importance based on recent events, specifically related to Russian interference in the 2016 national election. See the *Introduction and Background* section of this audit report for further information regarding the most recent United States Senate Intelligence Committee report released in July 2019 stating that voting systems in all 50 states were probably targeted in some manner.

The Department of State (DOS) is working with the Governor's Office of Administration, Office for Information Technology (OA/OIT) to develop a Request for Proposal to replace the SURE system given that it is over 15 years old. In a July 2019 report, the Brennan Center, a think tank within the New York University School of Law, interviewed DOS leadership and learned that "voter registration system replacement is absolutely about security."[61] It is imperative that DOS continue with its plans to develop and implement a replacement system to ensure the voter registration rolls are secure.

While conducting our audit procedures related to our audit objective to evaluate security protocols of the SURE system, we intended to test both security protocols, including cybersecurity controls implemented to protect the SURE system from outside cyber-attacks, as well as test information technology general controls (ITGC).[62] As described in *Finding 1*, however, DOS refused to provide us access to significant key documents related to the security, information technology (IT) controls, and operation of the SURE system.[63] Without these critical documents, we were unable to satisfy our audit objective to review the security protocols of the

[60] 25 Pa.C.S. § 1222(a), (c)(2), (c)(4), (c)(5), and (c)(14).

[61] Brennan Center for Justice. *Defending Elections: Federal Funding Needs for State Election Security*, <https://www.brennancenter.org/sites/default/files/publications/2019_07_DefendingElections_Final.pdf> (accessed July 31, 2019).

[62] ITGC are controls that apply to all systems, components, processes, and data for a given organization or IT environment. ITGCs must be designed and operating effectively in order to support the security of the systems, as well as to ensure application controls, such as edit checks, are operating effectively.

[63] As detailed in *Finding 1*, DOS contended that they were unable to provide outside security assessments and other detailed systems documentation because their election infrastructure was determined to be "critical infrastructure" by the US Department of Homeland Security (Homeland Security). However, DOS was unable to obtain confirmation of this position from Homeland Security. Further, during the course of the audit we learned that this type of information has been provided to auditors in other states. Further, DOS contended that they could not provide the information because it was against their policy. The policy in question, however, was not issued by DOS until April 23, 2019, *after* the deadline for providing documents for use during the audit.

SURE system and conduct our audit in accordance with applicable *Government Auditing Standards,* since the standards require auditors to evaluate the design and operating effectiveness of information systems controls when those controls are significant to the audit objectives.[64]

Based on the limited information that DOS management did provide to us or through review of other available information, we were able to identify gaps between leading IT security practices and the current policies, procedures, and practices protecting the SURE system and supporting architecture. Specifically, we found:

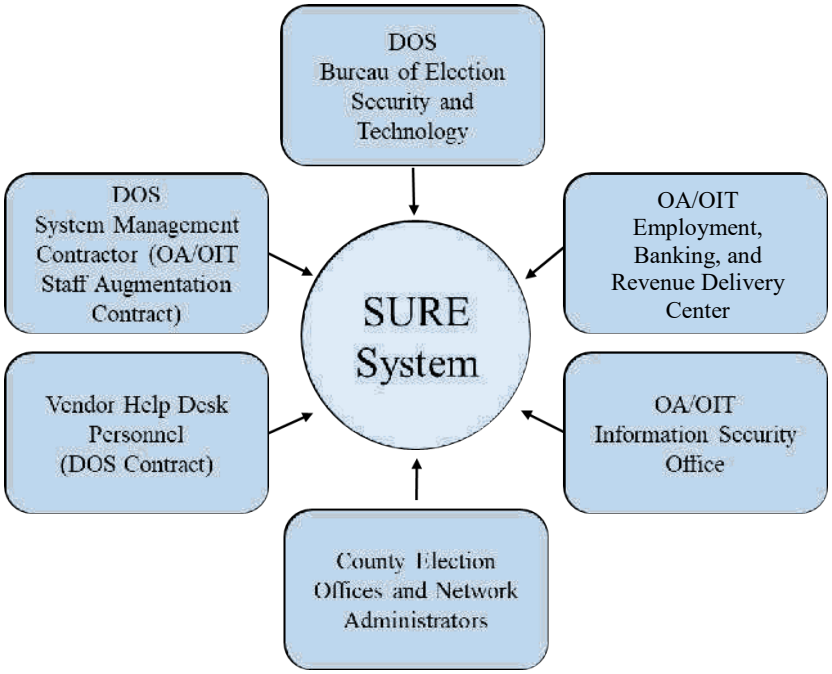
- The governance structure of the SURE system and supporting architecture does not adequately define oversight and IT management in order to implement effective IT controls.
- DOS management's vendor oversight practices need to be improved.
- DOS management's county-level *SURE Equipment Use Policy* fails to provide clear guidance to counties.

In addition, during our procedures we identified potential areas of improvement related to computer security, ITGCs, and interface controls that we have specifically excluded from this report because of the sensitive nature of this information. These conditions and our recommendations have been included in a separate, confidential communication to DOS management.

The governance structure of the SURE system and supporting architecture does not adequately define oversight and IT management in order to implement effective IT controls.

Since the implementation of the SURE system, DOS has worked with vendors, OA/OIT, and the county election offices (counties) to operate, maintain, and secure the SURE system and its supporting infrastructure. The following diagram provides an overview of the various individuals and organizations that must work together to operate, update, maintain, and secure the SURE system.

[64] U.S. Government Accountability Office. *Government Auditing Standards*. 2011 Revision. Paragraph 6.24 states that, "When information systems controls are determined to be significant to the audit objectives or when the effectiveness of significant controls is dependent on the effectiveness of information system controls, auditors *should* then evaluate the design and operating effectiveness of such controls." According to paragraph 215b, *Government Auditing Standards* uses the word *should* to indicate a presumptively mandatory requirement with which auditors must comply in all cases where such a requirement is relevant except in rare cases where auditors perform alternate procedures to achieve the intent of the requirement. In the case of the SURE audit, given the lack of documentation provided by DOS, no alternative procedures were possible.



Source: Produced by the Department of the Auditor General staff based on information provided by DOS management.

In April 2016, Governor Tom Wolf signed Executive Order 2016-06, assigning overall responsibility for the management and operation of IT services for all executive agencies to OA/OIT.[65] Under this Executive Order, most IT professionals in the various agencies were transferred to OA/OIT effective July 1, 2017. IT governance over the SURE system, however, has not been fully transferred to OA/OIT.

The governance structure of the individuals responsible for operation and maintenance of the SURE system includes multiple parties without defined, clear lines of authority between them. At the Commonwealth level, the Bureau of Election Security and Technology are DOS employees while most Commonwealth IT employees operating and maintaining the SURE system are OA/OIT employees. The Help Desk vendor operates under a contract with DOS, and the key IT system manager for many aspects of the SURE system is a contractor hired by DOS management through an OA/OIT staff-augmentation contract. With the counties also connected to the SURE system, the counties' systems and network administrators also have a part to play in the administration of the SURE system statewide. There is no single oversight body that coordinates all the parties and ensures an effective system of internal controls is in place that meets the needs of all stakeholders, including DOS management, the counties, OA/OIT, and registered voters of Pennsylvania.

[65] Executive Order 2016-06, *Enterprise Information Technology Governance*, dated April 18, 2016.

In addition, DOS was unable to describe or document the structure for responsibility and authority over the maintenance and operation of the SURE system and infrastructure. We requested a description of the working and reporting relationships of the various parties responsible for maintaining and securing the SURE system. DOS management was able to provide organizational charts for the technology groups in DOS and OA/OIT, and simply stated that there are no inter-organizational reporting relationships, but rather collaborative peer relationships.[66] We found this organizational structure unclear and were not provided with a document that would define authority and responsibility for these "collaborative peer relationships" described by DOS management.

The Commonwealth's standards over internal control state that management must establish an organizational structure, assign responsibility, and delegate authority in order to achieve its objectives. Additionally, the standards state the establishment of an oversight body to oversee its internal control system is foundational to effective internal controls and documentation of its internal controls systems must be adequate.[67]

Without a clearly defined governance structure and clear reporting relationships, silos of information may develop that could foster miscommunication and security gaps. It is imperative that the roles of an oversight body and IT management for maintaining and securing the SURE system be clearly defined in a governance document that provides guidance and structure to the organization. In the current high-risk environment, when outside actors have an interest in disrupting American elections and interfering with our democracy, clear lines of communication and authority are essential to timely and effectively responding to cyber threats and attacks.

DOS management's vendor oversight practices need to be improved.

DOS management relies on service organizations (vendors) for the operation and maintenance of key parts of the SURE system and its supporting infrastructure. These vendors were procured through contracts with other Commonwealth agencies, such as the Pennsylvania Department of Transportation (PennDOT) and the Governors' Office of Administration (OA), but provide services relevant to supporting the SURE system's operation and maintenance. Our procedures to review DOS's vendor management controls included requesting key vendors' System and Organization Control (SOC) reports, which are reports on a service organization's controls by an independent auditor. DOS management is required by Commonwealth policy to obtain and review vendor's SOC reports or perform other vendor monitoring when controls at the vendor

[66] DOS and OA/OIT use vendors, organizations working under an agreement with DOS or OA/OIT, to maintain and operate specific systems, as well as staff-augmentation contractors, hired to supplement Commonwealth employees, to perform similar functions as employees.

[67] The United States Government Accountability Office, *Standards for Internal Control in the Federal Government*, sections 2.01, 3.01, and 3.09. The Pennsylvania Governor's Office adopted these federal standards for all Commonwealth agencies within Management Directive 325.12, effective July 1, 2015.

are integral to the agency's system of internal controls.[68] Additionally, the Pennsylvania Department of General Services' (DGS) *IT Contracts Terms and Conditions* procurement policy requires that vendor contracts contain specific language regarding security, confidentiality, and audit provisions to aid in ensuring the security and confidentiality of the SURE system and data.

DOS management could not provide the SOC reports for service organizations or evidence that it reviewed the SOC reports and assessed whether controls at the service organizations were appropriately designed and operating effectively. In addition, DOS management could not provide evidence that they had reviewed any complementary user entity controls noted in the SOC reports and ensured that they were operating effectively at PennDOT and OA. Further, DOS management did not have the vendor contracts readily available for review and referred us to other Commonwealth agencies. Finally, DOS agreements with PennDOT did not require PennDOT's contracts with their vendors to include DGS's *IT Contract Terms and Conditions* to ensure the security of the SURE system and data.

Without adequate, documented monitoring of vendor controls and security practices, DOS management cannot be assured that the vendors are properly securing the SURE system and infrastructure.

DOS management's county-level *SURE Equipment Use Policy* fails to provide clear guidance to counties.

The *SURE Equipment Use Policy* (policy) imposes requirements on county users of the SURE system for appropriate use of the IT equipment provided by DOS management.[69] Specifically, this policy requires appropriate physical security for SURE system components located at the counties. The policy describes procedures for connecting county-owned equipment to the SURE system and prohibits the following:

- Installation of software on DOS-provided equipment.
- Use of SURE network equipment for non-SURE network traffic.
- Sharing user IDs and passwords.

[68] Management Directive 325.13, *Service Organization Controls*, establishes responsibilities for the oversight and evaluation of external parties (known as service organizations) likely to be relevant to an agency's internal controls, such as vendors that operate and maintain systems key to the SURE system. The Management Directive requires agencies to obtain and review SOC reports and/or perform other monitoring activities to understand the controls each service organization maintains, as well as how each service organization's internal controls system interacts with the agency's internal control system.

[69] During the audit, we received two versions of the *SURE Equipment Use Policy* with different dates and slightly different information, one version from a county and one version from DOS management. Further, we saw on the *SURE User ID Request Form* which must be signed by new SURE users, a reference to a policy entitled, *SURE User and Equipment Policy,* which was not provided for review.

The policy fails to include the additional responsibilities for security if the county chooses to connect county-owned equipment to the SURE system. The policy also fails to require use of a form to request and approve such deviations to track and monitor nonconformities from the preferred network architectural model or the use of county-owned equipment. Requiring the use of a form to request such changes would formalize the process for these deviations and provide a system for logging and monitoring associated risks.

DOS management did not provide us with the most recent (updated in 2012) version of the policy. We were unable to determine whether new users were provided the most recent version and whether county network administrators, who are responsible for maintaining the SURE system architecture but who might not be given SURE user IDs, are required to review and sign the policy. Further, the policy was referenced on the *SURE User ID Request Form* under another name, the *SURE User and Equipment Policy*, which may cause confusion among users. Finally, there is no master list of all SURE system policies applicable to the counties and their IT vendors which clearly specifies the most recent approved versions for each policy.

It is important that DOS management provide clear guidance to counties on the use, maintenance, and configuration of equipment connected to the SURE system, and it is vital that the SURE IT management team (DOS, OA/OIT, contractors, and vendors) continue to implement leading security practices, such as those specified in the recent *Best Practices for Securing Election Systems* document issued by the United States Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (DHS-CISA).[70] Without adequate security over the system, the voter registration rolls may be vulnerable to fraud, manipulation, deletion, and extraction by malicious actors who intend to disrupt elections across Pennsylvania. Ensuring leading practices are implemented and consistently documented will help to ensure the integrity of the voter rolls and facilitate efficient and fair elections.

Recommendations for Finding 3

We recommend that the Secretary of the Commonwealth:

1. Consider creating an oversight body to regularly meet about the SURE system consisting of members with SURE system knowledge, relevant expertise, and the appropriate independence needed to fulfill such oversight duties. The Secretary should consider appointing members that represent all key stakeholders of the SURE system including the counties and OA/OIT.

[70] <https://www.us-cert.gov/ncas/tips/ST19-002> (accessed May 23, 3019).

We recommend that DOS management:

2. Coordinate with OA/OIT to develop a governance structure that will provide clear lines of authority in operation, maintenance, and security of the SURE system and its supporting infrastructure. This control structure should address all parties with access to and/or responsibility for the SURE system and its supporting infrastructure and should be formalized in a governance document that is formally adopted by DOS and OA/OIT.

3. Continue with plans to replace the SURE system with a more up-to-date system that includes current leading security features.

4. Implement, along with OA/OIT, the security guidelines issued by DHS-CISA in May 2019, *Best Practices for Securing Election Systems*.

5. Ensure agreements with other agencies include requirements that vendors comply with all Commonwealth security policies and that the agencies update vendor contracts to include the most recent DGS *IT Contracts Terms and Conditions* for security, confidentiality, and audit provisions.

6. Monitor vendors through a documented process that complies with Management Directive 325.13, *Service Organization Controls*, including documented reviews of SOC reports.

7. Collaborate with PennDOT and OA/OIT to identify key contacts at each agency and delivery center who would provide oversight and evaluation of each service organization's internal controls. Specific consideration should be given to the following:

    a. Timely reviewing SOC reports and documenting the assessment of the review.

    b. Reviewing SOC reports for noted exceptions that may affect DOS processes and following up with the vendor's corrective action plans.

    c. Reviewing SOC reports' complementary user entity controls to ensure those controls are in place and operating effectively at agencies and/or applicable sub-service organizations.

    d. Ensuring SOC report results are communicated to all affected agencies and escalation procedures exist when the report(s) includes control objective exceptions, testing deviations, or a qualified opinion.

8. Update the *SURE Equipment Use Policy* to address the risk of counties connecting county-owned equipment to the SURE system or deviating from the preferred architectural model.

9. Consider instituting the use of a form for counties to request and receive approval from DOS for deviations from the approved network architectural model or the use of county-owned equipment.

10. Ensure that all county users, including county administrators and vendors, review and sign an updated version of the *SURE Equipment Use Policy*.

11. Correct the reference to the *SURE User and Equipment Policy* on the *SURE User ID Request Form* to eliminate confusion as to policy requirements applicable to county users of the SURE system.

12. Create a master list of all SURE system policies applicable to the counties and their IT vendors, which clearly specifies the most recent approved versions for each policy.

Finding 4 – Voter record information is inaccurate due to weaknesses in the voter registration application process and the maintenance of voter records in the SURE system.

The Help America Vote Act (HAVA) outlines minimum standards for the accuracy of voter registration records and requires states including Pennsylvania, to perform list maintenance on a regular basis to remove ineligible voters and voters who have not: (1) responded to a notice; and (2) have not voted in two consecutive general elections for Federal office.[71]

Pursuant to HAVA, each State acting through its chief state election official (for Pennsylvania this is the Department of State (DOS)), must:

> Implement a single, uniform, official, centralized, interactive computerized statewide voter registration list defined, maintained, and administered at the State level that contains the name and registration information of every legally registered voter in the state.[72]

DOS' implementation and use of the Statewide Uniform Registry of Electors (SURE) system, as discussed throughout this report, is intended to fulfill this requirement. Based on our audit procedures covering the period January 1, 2016 through April 16, 2019, it appears that DOS and county election offices (counties) generally utilize the SURE system as designed. The counties perform list maintenance on voter records in order to attempt to comply with federal and state laws. We found, however, that the SURE system and supporting processes and controls (collectively Pennsylvania's voter registration process) are not effective to ensure that voter registration information is accurate. Based on federal and state law, accuracy with regard to voter registration information includes the following:

- Only eligible voters are registered to vote.
- All information fields within voters' records agree with information provided on the application form.
- All applications are timely processed to ensure information is current.
- Each voter has one unique record.

[71] *See* 52 U.S.C. § 21083, including Subsection (a) "Computerized statewide voter registration list requirements" and Subsection (a)(4) "Minimum standard for accuracy of State voter registration records."
A notice is correspondence mailed by a county election office to a voter requesting the voter to confirm their address. A notice is mailed due to either the individual not voting for five consecutive years or information the Department of State obtains from the United States Postal Service regarding a potential change of address for the voter. For the purpose of this audit, a "voter" is a person who is registered to vote in Pennsylvania. It does not indicate that the person has voted in an election.
[72] 52 U.S.C. § 21083(a)(1)(A).

- Each voter is assigned the correct voting status, e.g., *active versus inactive*.[73]
- All ineligible voters are removed from the registration rolls in a timely manner.

Inaccuracies presented in *Finding 2*, as well as information discussed later in this finding, demonstrate that Pennsylvania's voter registration process does not adequately ensure that the voter registration information within the SURE system is accurate.

Based on our audit procedures, we identified several reasons why inaccuracies occur within Pennsylvania's voter registration process. This finding categorizes reasons into the following two areas, noting where each reason is discussed within the report after each listed item:

- Weaknesses within the voter registration application (application) process.
- Weaknesses regarding the maintenance of voter registration records (list maintenance) within the SURE system.

Weaknesses within the application process

- No review is required to ensure that data on the application form is being accurately entered into SURE either at the time of data entry or on a routine basis after data entry. (See below)
- Automated edit checks and other features that would prevent or detect inaccuracies are not sufficiently incorporated into the SURE system. (See *Findings 2 & 5*)
- The process to search for duplicate records is predominately a manual process and is inadequate. (See *Finding 2*)
- County staff added a generic date of birth (DOB) (e.g., January 1, 1900) in the SURE system for thousands of voters when the counties migrated their data into the SURE system upon implementation between 2003 and 2005 and never corrected those dates. (See *Finding 2*)
- Applications remain in pending status for long time periods, indefinitely in some cases. (See below)
- The source documents for some voter record information have not been maintained by the counties due to a lack of clear record retention guidance. (See *Finding 6*)

Weaknesses regarding the maintenance of voter registration records within the SURE system

- Although list maintenance activities are performed by counties, insufficient analysis and monitoring has resulted in inaccurate data in the voter records. (See below)

[73] A voter in active status can vote after signing the poll book at their polling place. A voter is to be placed in inactive status if they have not voted nor had any communication with the county election office in at least five years. An inactive voter is still able to vote but will need to sign an affidavit to confirm their continued eligibility at their polling place before casting their ballot.

- Voters who should be classified as inactive or whose records should be cancelled according to state law remain in an incorrect status within the SURE system. (See below)
- The process to search for deceased voters is predominately a manual process and is inadequate. (See *Finding 2*)
- DOS does not fully utilize the list maintenance feature it pays for as a member of the Electronic Registration Information Center (ERIC).[74] (See below)

The following sections describe the weaknesses within the application process and the maintenance of voter registration records within SURE that are not presented in other findings.

Weaknesses within the application process

As part of our audit procedures, we visited seven counties to gain an understanding of how the counties process applications in SURE, including procedures for applications received electronically and for applications received in paper format. Our analysis included the procedures for both new applications and updates to voter records.

For paper applications, county staff manually enter all of the application information into SURE. Applications electronically received, either online or through the Pennsylvania Department of Transportation (PennDOT) Motor Voter system, require less manual input from staff. While there are times when county staff may need to make edits to the information, such as moving data to the correct field, generally speaking, the data entry part is completed by the applicant.[75] County staff only need to review to ensure that the required information is present, conduct duplicate voter record checks (discussed in *Finding 2*), and assign the voter to the correct precinct.

Whether the applicant submits an application in paper format or electronically through DOS' website as part of the application process, the SURE system requires county staff to run a mandated HAVA check prior to completing the registration process.[76] The HAVA check compares the applicant's information supplied on the application to either the information maintained by PennDOT or the U.S. Social Security Administration. These comparisons are only performed if the individual has provided either a Pennsylvania driver's license (DL) or Pennsylvania identification (ID) number and/or the last four digits of their Social Security number (SSN).[77] Providing this information on the application is not mandatory. If the

[74] ERIC is a non-profit corporation governed by a board of directors made up of member-states, including Pennsylvania. https://ericstates.org/who-we-are/ (accessed August 12, 2019).
[75] An example of an edit that may be required is if the house number is located in the field for the street name rather than the field for the house number.
[76] 52 U.S.C. § 21083(a)(5) "Verification of voter registration information."
[77] The HAVA check includes: checking the applicant's first two characters of last name in conjunction with the PennDOT DL or ID number and DOB, if the applicant supplied their DL or ID number. If the applicant supplied the last four digits of their SSN, the check includes: checking the applicant's last name, first name, middle initial, last

information provided on the application matches the HAVA check results, the registration is automatically approved. If any of the information provided on the application does not match and the county staff confirms that in the case of paper copy applications that there was not a data entry error, the application is placed in pending status (discussed later in this finding). At this point, a HAVA non-match letter is generated through SURE that the county mails to the applicant requesting clarification of the information provided.

No review is required to ensure that data on the application form is being accurately entered into SURE either at the time of data entry or on a routine basis after data entry.

Based on our audit procedures, neither DOS nor the SURE system itself require counties to have a second person, whether a colleague or supervisor, to double-check the accuracy of data entry performed so that typographical errors can be immediately corrected at the time the applications are processed. According to our survey results, at least 35 of the 65 counties that responded have two or fewer people in the elections office, which could make a required second person or supervisory review process difficult.[78] We understand that during peak processing times it may not be practical for counties to double-check data entry accuracy for application processing; however, this does not negate the risk that data entry errors will likely occur. Efforts should be made to mitigate this risk by routinely reviewing the data entry information as frequently as possible to detect and correct typographical errors.

Based on our discussion with DOS management, we also found that DOS does not provide guidance to counties regarding reviews of data entry information to ensure accuracy. Based on responses from the survey however, we found that some counties have implemented their own rules for reviewing data entered into SURE for applications. As part of the survey, we asked county directors if they reviewed work performed in SURE by county staff to help ensure accuracy of voter records.[79] Only 35 of the 64 counties (less than 55 percent) that responded to this particular question indicated that they review work performed by county staff in SURE. The responses regarding the frequency of reviews conducted included comments such as, "as needed," "as time allows," "monthly," "weekly," and "daily." One county indicated that its staff performs a weekly review of voter information to determine if there are any records with duplicate DL numbers, names, DOB, and addresses. In addition, the same county indicated that a monthly review is performed to determine if any records are missing party affiliation or precinct designation.

---

four digits of the SSN, and DOB. An applicant can indicate on their application that they do not have a DL, ID or SSN. As with all first time voters, the applicant must show one form of approved identification (see list in *Appendix C*) when voting for the first time.

[78] The information is based upon responses from the counties in the county survey performed as part of our audit procedures. See *Appendix H* for a copy of the survey sent to the counties.

[79] A total of 65 of the 67 counties provided responses to our questions either during the on-site interviews or by returning the survey; however, not all of the counties responded to every question in the survey.

Due to staff limitations in some counties, it may not be feasible for every county to conduct weekly checks; however, routine reviews and data analysis would help to identify missing and inaccurate data as well as ensure the accuracy of the voter records maintained in SURE. See *Finding 2* for details on our data analysis results that indicates thousands of potentially inaccurate voter records exist.

In addition to the counties performing periodic reviews of voter information, it would be beneficial for DOS to analyze voter information data on a statewide basis for accuracy and reasonableness. When inaccurate data is entered into SURE, other procedures designed to keep the SURE system accurate, such as the duplicate check, cannot work effectively because exact matches are less likely. Therefore, DOS and counties should be performing periodic analyses of the voter information data for missing and/or inaccurate data.

In addition to DOS and counties performing internal reviews of the data in SURE, another available option is for DOS to contract with a third-party vendor to review the data and perform an analysis. Such an analysis would be similar to that performed during our audit procedures to identify potentially inaccurate or missing data in voter records for DOS and/or counties to investigate and resolve.

Applications remain in pending status for long time periods, indefinitely in some cases.

Applications (both initial applications and applications to update existing voter record information such as name, address, political party) received by the counties that are missing required data, such as personal information, party selection, or a signature, are placed into a pending status in SURE. DOS management stated that counties are to follow-up with the applicant and request the missing information in order for the application to be processed. Additionally, if the HAVA check portion of the voter registration process results in a non-match, the application is placed into pending status while awaiting follow-up with the applicant.

According to DOS management, there is currently no criteria established requiring counties to follow-up or reject an application that remains in pending status after a certain amount of time has elapsed (this issue is further discussed in *Finding 7*). Based on data analysis, as of October 9, 2018, there were 91,495 applications in pending status, including applications from all 67 counties.[80] The following table provides a summary of the applications in pending status as of October 9, 2018, based on the age of the pending record:

[80] According to interviews with both DOS and county staff, work to clear applications from pending status occurs up through each election, which in this case was November 6, 2018. County staff therefore had approximately one month from October 9, 2018 through November 6, 2018, to further process the applications and potentially remove some from pending status.

Applications in Pending Status[81] As of October 9, 2018		
Number of Months/Years the Application had been in Pending Status	**Number of Applications**	**Percent**
0 to 30 days	25,022	27.35%
31 to 180 days	7,958	8.70%
181 to 365 days	3,738	4.09%
12 to 24 months	12,639	13.81%
24 to 33 months	18,932	20.69%
Subtotal: Number of applications placed in pending status during our audit period (January 1, 2016 forward)	**68,289**	**74.64%**
33 months to 4 years	4,498	4.92%
4 to 6 years	3,396	3.71%
6 to 8 years	3,526	3.85%
8 to 10 years	4,235	4.63%
More than 10 years	7,551	8.25%
Subtotal: Number of applications placed in pending status prior to the beginning of our audit period (January 1, 2016)	**23,206**	**25.36%**
Total	**91,495**	**100.00%**

Source: This table was compiled by the staff of the Department of the Auditor General from data received from the SURE system. We determined that the reliability of this data had significant limitations in regards to completeness and accuracy as noted in Appendix A. Although this determination may affect the precision of the numbers we present, there is sufficient evidence in total to support our findings and conclusions.

As reflected in the above table, a record can remain in pending status indefinitely. More than 7,500 applications have been in pending status for more than 10 years. DOS management stated that they have asked counties to review pending applications and reject them, if appropriate. Based on the number of pending applications, it does not appear that counties have made the cancellation of older pending applications a priority.

Further, it appears that many of the applicants with records in pending status have submitted subsequent applications (either a new request to register to vote or to update their existing voter record information) which would potentially make the prior pending application moot. We found 16,000 pending records that matched a subsequent application filed by the same voter.

Based on additional analysis performed, we determined that almost 95 percent of the 68,289 applications placed into pending status during our audit period, or 64,587, were awaiting a response from the applicant in order to further process the application while approximately 5 percent required action by the county to complete processing.

[81] A list of these records has been provided to DOS to allow them to instruct the county election staff to review the records and make a determination as to whether they should be processed further or rejected.

Of the 64,587 applications that were awaiting a response from the applicant, 16,206 were pending while awaiting a response from the applicant who was sent a HAVA non-match letter. DOS management stated that there is no legal basis under federal or state law to reject or delay the processing of a voter registration application based solely on a HAVA non-match. Therefore, for these 16,206 applications, county election staff is responsible for making a determination as to whether there are grounds for rejection or if the applications should be processed for approval.

When an individual's application is placed in pending status due to the applicant not providing all required information, they are sent a letter explaining the deficiency and requesting the missing information. When an individual's application is placed in pending status because it requires action by the county to continue processing, it is possible that the applicant may be unaware that their registration has not been approved, and therefore is not eligible to vote. We believe that the number of applications in pending status would be drastically reduced if guidelines existed requiring counties to: (1) take action within a certain time period on applications that require further review or processing by the county, and (2) reject incomplete applications if the applicant does not respond to the county's inquiry within a certain timeframe. If an application must be rejected, a notice would be mailed to the applicant. This would help to ensure that the applicant is notified that they have not been registered and therefore are unable to vote. Once rejected, an individual has the ability, if they so choose, to again register to vote, which would start the process again. We believe, and DOS management agreed, that it is better for an individual to have their registration rejected than to have it remain in indefinite pending status. DOS should work with its legal office to determine whether the above-suggested guidelines can be implemented.

Weaknesses regarding the maintenance of voter registration records within the SURE system

Pennsylvania voter registration laws require the maintenance of a database containing records for all registered voters. It also requires that the database permit the sending of notices regarding death, change of address, or other information affecting the qualifications of an applicant or registration of a registered voter, and identify duplicate voter registrations on a county and statewide basis.[82] State law also requires the removal of voters and use of National Change of Address (NCOA) on a periodic basis, but not less than once every calendar year, to identify registered voters who may have changed addresses.[83] These requirements are to help ensure that voter records for individuals who are no longer eligible to vote are cancelled in a timely manner and that voter records are properly updated for those voters who have moved to a new county.

[82] Pennsylvania Voter Registration Law (PVRL) – 25 Pa.C.S. §§ 1201(3) and 1222(c). See also 25 Pa.C.S. § 1901(b) "Voter removal program."
[83] Ibid. at 25 Pa.C.S. § 1901(b).

Federal and state election law governs the election cycle in Pennsylvania.[84] Each county must complete specific tasks, such as completing list maintenance activities no later than 90 days prior to the general election in order to comply with these laws. List maintenance of the computerized list must be performed on a regular basis and must be conducted in a manner that ensures that:

- The name of each registered voter appears in the computerized list.
- Only voters who are not registered or who are not eligible to vote are removed from the computerized list.
- Duplicate names are eliminated from the computerized list.[85]

As noted in the *Introduction and Background* section, elections in Pennsylvania are a function of local elections offices. DOS, however, also has certain authority over the state's elections. The counties own the voter registration records, but federal law placed the requirement to create and maintain the SURE system with DOS. DOS must ensure that voter registration records are accurate and are updated regularly. As a result, DOS provides oversight to the counties to ensure that they complete all required tasks in accordance with the governing law, but DOS does not have any authority over the counties, which are governed by county commissioners or a county executive. There is a delicate balance between DOS and the counties. DOS needs the counties to do what they are statutorily required to do, but lacks the power to mandate compliance or to simply do the required work itself.

The following sections describe the weaknesses we found related to the maintenance of voter registration records.

Although list maintenance activities are performed by counties, insufficient analysis and monitoring has resulted in inaccurate data in the voter records.

During our review of DOS reports, analysis of SURE data, and testing performed on voter records, we saw evidence that counties had performed required list maintenance activities on voter records.[86] The annual report presented by DOS to the Pennsylvania General Assembly includes information, by county, of the number of voters affected by list maintenance activities. DOS also provided us with examples of emails between the Help Desk and DOS staff regarding county progress in conducting list maintenance, such as the number of voter records given to a

[84] Help America Vote Act (HAVA) – 52 U.S.C. § 21083(a)-(b); PVRL – 25 Pa.C.S. §§ 1201(3), 1222(c), and 1901(b)(1)(i).
[85] 52 U.S.C. § 21083, Subsection (a)(2) "Computerized list maintenance" and Subsection (B) "Conduct." Pennsylvania election law assigns the responsibility of maintaining voter records to the county election offices.
[86] List maintenance activities are prescribed by law and are performed by counties to help ensure that the voter rolls remain up to date and accurate. Such activities include an annual change of address mailing and a five year mailing to voters who have not voted in two federal general elections. *See* 25 Pa.C.S. § 1901(c) and (d).

county to follow up regarding the NCOA process and how many of those voters were sent correspondence, confirming follow-up was performed.[87]

Additionally, we analyzed the data in the application table from the SURE system to look for indications that counties performed list maintenance activities as required by federal and state law.[88] The results of our testing indicated that all 67 counties had updated voter records for list maintenance activities and, therefore, had performed some type of list maintenance during the audit period January 1, 2016 through October 9, 2018. Based on information contained in the SURE system, there were indications that all 67 counties had updated records for change of address, deceased individuals, and inactive voters. Virtually all counties' data had indications of list maintenance activities in each of 2016, 2017, and through October 9, 2018.[89] There are limitations in the data received from the SURE system that prevent a high level of assurance in the data analysis results; however, the data appeared to corroborate DOS management's statement that all counties performed required list maintenance activities annually during our audit period.[90]

Additionally, as part of our audit procedures, we visited seven counties between July 11, 2018 and September 11, 2018. The NCOA mailings (a required list maintenance activity) are typically conducted during the summer when the counties are between election cycles. During our visits we observed counties processing responses to the NCOA mailings, which further verifies that they conducted the NCOA process.

While the above scenarios appeared to corroborate DOS management's assertion that all counties perform the required list maintenance, the effectiveness of the list maintenance activities is largely based on the accuracy of the existing voter records. As explained in *Finding 2*, insufficient analysis is being performed to identify duplicate voters during the application process and to identify all deceased voters on the voter rolls. Issues also exist with the accuracy of voter records, including missing or incorrect birthdates, duplicate records, and potentially deceased voters that remain on the voter rolls. As the list maintenance process is dependent upon

---

[87] The NCOA includes mailing a notice to each voter that was identified as having possibly moved in the last year. The data is provided to DOS by ERIC.

[88] The application table contains the history of all additions and changes made to voter registration records since the implementation of the SURE system in 2003 through 2005. Each change to a voter registration record is captured as a record in the application table. *See* 52 U.S.C. § 21083(a)(2) "Computerized list maintenance" and 25 Pa.C.S. § 1901(b) "Voter removal program."

[89] The application table data for one small county that contained only four list maintenance records in 2017 contained no list maintenance records in 2016. We deemed the level of list maintenance activity reasonable for that small county. The data also included no indication of list maintenance performed by one other county during approximately the first nine months of 2018 (January 1, 2018 through October 9, 2018, the date our data was extracted by DOS), but there was still time for that county to complete its list maintenance activities by the end of calendar 2018.

[90] We determined that the reliability of this data had significant limitations regarding completeness and accuracy as noted in *Appendix A*. Although this determination may affect the precision of the numbers we present, there is sufficient evidence in total to support our findings and conclusions.

accurate voter record data in order to identify individuals, until the inaccurate voter record information is corrected, the list maintenance activities will only be marginally effective.

DOS management stated that it regularly monitors the work performed by counties; however, it does not have standard operating procedures formalizing the monitoring conducted, nor does it monitor whether the work by the counties is adequately performed.[91] DOS management stated that there are multiple DOS staff members who regularly receive emails from the Help Desk that update them on the status of work performed in SURE by each county. DOS management provided us with examples that included daily automated emails indicating if list maintenance processes have been completed, what counties have certified their voter registration statistics, and what counties have started/completed printing their poll books for an election. There are no written procedures, however, to document the frequency and which staff members are ultimately responsible for monitoring the various types of work performed by the counties. Additionally, DOS staff does not maintain a centralized document to track the status of work performed by each county. As a result of DOS staff not maintaining a centralized document, DOS is unable to document the work done to track the status of the counties' work in order to determine if there are any county election offices that need to be notified/reminded of required work necessary to meet established deadlines or confirm that all required tasks have been completed by each county. Therefore, we could not confirm that DOS regularly monitored each county for required tasks.

It is imperative that standard operating procedures be formalized to ensure that there is clear direction on when and what monitoring is to be performed of the counties, as well as who at DOS is responsible for performing the monitoring. Both DOS and counties must work together to ensure that all processes are completed in a timely manner so that all eligible persons who have applied to register to vote are allowed to vote.

Voters who should be classified as inactive or whose records should be cancelled according to state law remain in an incorrect status within the SURE system.

State law requires that voters without any activity for five years be placed in inactive status.[92] In order to test that all counties were performing list maintenance activities to identify inactive voters, we performed data analysis to look for voters who should have been changed to inactive status based on the required criteria. We identified 96,830 active registered voters who had no activity in the past five years (e.g., they did not vote, did not change their address, did not change

[91] Examples of county work that DOS monitors includes ensuring applications are being processed, list maintenance is being performed, poll books are printed timely prior to an election, and that voter registration statistics are certified.

[92] As defined in **Pennsylvania Voter Registration** Law (PVRL) (Act 3 of 2002), 25 Pa.C.S. § 1901(c), registered voters are to be identified as inactive when they have not responded to a mailed notice from the county based on information received by either DOS or the county that a registered voter has moved. Additionally, the law indicates that registered voters should be identified as inactive when they have not responded to a mailed notice from the county when they have not voted within the last five years.

political party, etc.). These voter records likely should have been placed into inactive status by counties when performing required list maintenance procedures unless there was some form of communication between the county and voter that was not included in the data we analyzed. As reported in the following table, almost 44 percent of the total 96,830 stale, but still active, voter records were voters registered in Allegheny County:[93]

Active Registered Voters as of October 9, 2018 with no Activity During the Period October 9, 2013 through October 9, 2018 (Five Years with no Activity) by County		
County[a/]	**Number of Voters**	**Percentage of Total Voters**
Allegheny	42,437	43.83%
Cumberland	13,215	13.65%
Luzerne	7,395	7.64%
Northumberland	6,164	6.36%
Philadelphia	6,280	6.48%
48 counties	21,339	22.04%
Total	**96,830**	**100.00%**
[a/] - Our analysis did not find any stale voters in 14 of the 67 Pennsylvania counties.		

Source: This table was compiled by the staff of the Department of the Auditor General from data received from the SURE system. We determined that the reliability of this data had significant limitations in regards to completeness and accuracy as noted in Appendix A. Further, we used the "date last voted" field, in part, for this analysis. As noted in Appendix A, this field is of undetermined reliability. Although these determinations may affect the precision of the numbers we present, there is sufficient evidence in total to support our findings and conclusions.

The law also requires that voters who have already been placed into inactive status and who fail to vote in the following two federal general elections should have their voter record cancelled.[94] Using our data analysis procedures, we found that 17 of the 67 counties had a total of 65,533 records of inactive registered voters who had not voted since the 2008 federal general election and therefore should have been cancelled, but remained registered in inactive status as of October 9, 2018. The following table provides detail regarding the four counties that account for 60 percent of these inactive registered voters and the amount of voters from the remaining 13 counties:

[93] For purposes of this finding, we consider a stale voter record to be voters that we identified as being in active status in spite of meeting the criteria to be moved to inactive status.
[94] PVRL (Act 3 of 2002), 25 Pa.C.S. § 1901(d)(1)(ii)(B).

Registered Voters who had been Inactive from 2003 through 2008 and who had Not Voted since the 2008 Federal Election but who had Not Been Cancelled as of October 9, 2018, by County		
County	**Voters**	**Percentage of Total Voters**
York	13,520	20.63%
Erie	9,873	15.07%
Allegheny	9,098	13.88%
Westmoreland	7,404	11.30%
13 other counties	25,638	39.12%
Total	**65,533**	**100.00%**

Source: This table was compiled by the staff of the Department of the Auditor General from data received from the SURE system. We determined that the reliability of this data had significant limitations in regards to completeness and accuracy as noted in Appendix A. Further, we used the "date last voted" field for this analysis. As noted in Appendix A, this field is of undetermined reliability. Although these determinations may affect the precision of the numbers we present, there is sufficient evidence in total to support our findings and conclusions.

Possible reasons for the counties' failure to move stale voters who meet the applicable criteria to inactive status or to cancel inactive voters' records could vary from simple oversight to not being able to complete list maintenance activities due to several special elections.[95] We did not conduct interviews with representatives from each county, and therefore did not determine the actual reasons. In failing to properly classify active voters as inactive and subsequently removing inactive voters from the voter rolls after the established time periods, counties are not complying with state law and are increasing the risk of fraudulent voting. In addition, since current controls to identify and remove deceased voters' records (discussed in *Finding 2*) appear to not be functioning in all cases, removal of inactive voters' records becomes more important as a safeguard against deceased individuals' voting records remaining active. In addition to these concerns, inaccurate voter rolls could also affect other voting related aspects, such as the size of an election district, which should not contain more than 1,200 registered voters, and the amount of funding for elections, including funding for voting machines, which is based on the number of eligible voters by county.[96]

As discussed throughout the finding, inaccurate information associated with a voter's record can inhibit a county's ability to keep their rolls up to date. As previously mentioned, list maintenance depends on the ability to match information provided for individuals to voter registration records. If information in a voter registration record is inaccurate, county election staff may erroneously disregard the information as not being a match to an existing voter record, which allows

[95] A special election is scheduled by the General Assembly in order to fill a vacancy due to the current elected official no longer being able to hold office such as due to death or retirement. Pursuant to the National Voter Registration Act (NVRA), 52 U.S.C. § 20507(c)(2)(A), and the PVRL (Act 3 of 2002), 25 Pa.C.S. § 1901(b)(4), a voter's record cannot be cancelled due to list maintenance within 90 days of an election.

[96] Pennsylvania Election Code Act of June 3, 1937, P.L. 1333, No. 320 Article V, § 502 "Court to Create New Election." *See* 25 P.S. § 2702, as amended. https://www.legis.state.pa.us/WU01/LI/LI/US/PDF/1937/0/0320..PDF (accessed June 7, 2019). Letter from DOS to the U.S. Election Assistance Commission with their narrative of how they will distribute the HAVA money. https://www.eac.gov/havadocuments/PA_narrative_Budget.pdf (accessed June 10, 2019).

duplicate voters to be included in the voter rolls. Inaccurate information can also result in a failure to cancel an ineligible voter's record, such as a voter who has died. Beyond the fact that the law requires that the voter rolls be maintained to include accurate information, accurate, up-to-date voter rolls are helpful to the voters by minimizing disruption at the polling places due to inaccurate information in the poll books.

DOS does not fully utilize the list maintenance feature it pays for as a member of ERIC.

As previously described, it is critical that accurate voter records be maintained. Organizations such as ERIC have been established to help improve the accuracy of America's voter rolls and increase access to voter registration for all eligible citizens.[97] From the launch of ERIC in 2012 through the end of 2017, ERIC helped its member states identify 8.4 million inaccurate voter records.[98] ERIC provides its member states with reports on voters who have moved in-state or out-of-state, voters who have died, voters with duplicate registrations in the same state, and individuals who are potentially eligible to vote but are not registered. According to DOS management, however, it only uses ERIC to obtain information for list maintenance purposes regarding change of address and is not utilizing available information such as death notices and cross-state matches.[99] We inquired of DOS management as to why they are not fully utilizing all of the features available through ERIC. DOS management responded that they "have plans to incorporate them into production prior to the November 2019 election." This is despite the fact that DOS has paid for but not utilized some of the information available to ERIC members since it first joined in 2015.[100]

Conclusion

Issues with the input of voter record data and the lack of fully performing list maintenance has resulted in inaccurate information being maintained in SURE. Additionally, by not updating voters' information and not removing ineligible voters from the voter rolls, counties are not complying with required state and federal laws. Finally, DOS is not utilizing benefits that it is paying for as a member of ERIC to aid counties with list maintenance procedures.

[97] ERIC 2017 Annual Report. https://ericstates.org/wp-content/uploads/2019/01/FINAL_ERIC_2017_Annual_Report.pdf (accessed March 25, 2019).
[98] Ibid. Pennsylvania, through DOS is one of 26 states, plus the District of Columbia that is a member of ERIC.
[99] Cross-state matches involve matching Pennsylvania voter records to out-of-state voter registration commissions and Department of Motor Vehicle records that indicate updated information.
[100] According to ERIC's web-site, each member pays a one-time membership fee of $25,000 and an annual fee. https://ericstates.org/wp-content/uploads/2019/01/ERIC_Bylaws_2018-11-30.pdf (accessed August 5, 2019).

Recommendations for Finding 4

We recommend that DOS:

1. Emphasize to the counties the vital need and importance of having a second person review the data entered into SURE to reduce data entry errors and increase the accuracy of voter records.

2. Consider supplementing the data analysis that we recommend DOS perform in *Finding 2* (Recommendation 2), by contracting with a third-party vendor to periodically perform analysis on the data in SURE to identify potentially inaccurate or missing data for DOS and/or counties to investigate and resolve.

3. Request that its designated legal counsel make a determination as to whether DOS can: (1) direct the counties to review their pending applications and reject them; and (2) establish a time period for requiring counties to process, or reject if applicable, all applications placed into pending status.

4. Instruct the counties to review the applications in pending status to determine if another application for the person has been approved which would then lead the county to reject the initial application currently in pending status.

5. Develop detailed written procedures, including detailed processes to be performed and by whom, regarding DOS monitoring the activities of the counties to ensure required processes are completed properly and timely.

6. Instruct the counties that have not been updating the status of voters from active to inactive, for those voters who meet the criteria of an inactive voter, to perform list maintenance and update voters' status as necessary. This instruction should include a deadline to be established by DOS. Additionally, formally remind all counties of the importance of why they need to perform this type of list maintenance.

7. Instruct the counties that have not been cancelling the records of the inactive voters who meet the criteria for cancellation to perform list maintenance and update voters' status as necessary. This instruction should include a deadline to be established by DOS. Additionally, formally remind all counties of the importance of why they need to perform this type of list maintenance.

8. Move forward with plans to utilize all information available from ERIC to assist in improving the accuracy of voter registration records.

Finding 5 – Incorporating edit checks and other improvements into the design of the replacement system for SURE will reduce data errors and improve accuracy.

Accurate voter information within voter registration systems is critical for two important reasons: (1) to ensure that only the voter registration applications (application) of individuals eligible to vote are approved and (2) only eligible voters are casting votes in elections. Because the Statewide Uniform Registry of Electors (SURE) system has been in place for more than 15 years, Pennsylvania Department of State (DOS) management stated that it has engaged the SURE Advisory Board to start discussing a replacement system. Additionally, DOS has started to develop the requirements and a timeline for the request for proposal process to replace the current SURE system. According to DOS management, the replacement system will be customized to meet the specific needs of Pennsylvania. As a result, the audit objectives included reviewing efficiencies of the SURE system that DOS should consider in the design of the replacement system to improve the processing of applications and improve accuracy.

As discussed in *Finding 4*, DOS does not require supervisors at county election offices (counties) to verify the accuracy of the application information manually entered into SURE by county staff. According to the survey we conducted, we found that less than 55 percent of the counties that responded to the survey perform any procedures to verify whether the application data was entered accurately.[101] In addition to manually verifying data entry accuracy, there are several information system input controls that could be utilized to increase the accuracy of the information entered into SURE. For example, edit checks for reasonableness, validity, and completeness tests can be programmed into the system to ensure certain data entry mistakes are detected/flagged by the system upon entry, which could then be immediately corrected by county staff at the time of data entry.[102]

Through our data analysis, we found instances where edit checks were lacking or non-existent. The following issues were previously discussed in *Finding 2*:

- The automated check for duplicate voter records within the SURE system at the time of application approval is inadequate.

[101] As part of our audit procedures, we sent a survey to all 67 Pennsylvania counties. 65 of the 67 counties provided responses to our questions either during on-site interviews or by returning the survey, however not all of the counties responded to every question in the survey. See *Appendix H* for a copy of the survey.

[102] An edit check is a type of data validation routine built into a system that is designed to ensure data input into the system meets certain criteria prior to being accepted into the database. There are a number of validation types that can be used to check the data being entered such as spell checks, presence checks (checks to make sure data is present in all required fields), or length checks (checks to make sure data is not too long or too short). Edit checks that could be used on voter application data could be a validation routine ensuring the voter will be at least 18 years of age by the date of the next election and ensuring the date of birth field includes only numbers and not letters.

- There are no automated edit checks in the SURE system that prevent adding a voter registration record with a driver's license (DL) number that is already associated with a voter record.
- There are no automated processes in the SURE system to prevent the recording of obviously inaccurate birthdates and/or voter registration dates, e.g., voter registration dates prior to date of birth (DOB).

We also found features that were missing or inadequate within the SURE system which could reduce or prevent errors. Specifically, we found:

- The SURE system does not prevent applications with non-Pennsylvania residential addresses from being approved.
- The SURE system lacks geographical mapping assistance which would reduce inefficiencies and potential inaccuracies by preventing applications from being sent to the wrong county for processing.
- The SURE system lacks a "Read Only" feature for voter information that should not be edited without additional supervisory review and approval.
- The SURE system does not have controls in place to ensure that voter registrations are not improperly cancelled within 90 days of an election.

In addition to these features, we were informed of two areas related to the Pennsylvania Department of Transportation (PennDOT) Motor Voter process and the reporting capabilities within the SURE system that need improvement:

1) Some individuals confuse the change of address prompt at PennDOT's photo license centers with registering to vote.
2) The ability to create reports in the SURE system is too limited and it lacks editable report capabilities.

It is clear that the SURE system itself needs to be improved, and there is a need for the counties to strengthen their oversight of the SURE system transactions and the accuracy of the data. DOS should conduct periodic reviews of the data to identify errors, inaccuracies, and omissions and instruct the appropriate counties to fix the identified issues. Incorrect data within SURE could lead to an individual being able to vote more than once in an election or for eligible voters to encounter difficulties, such as not being included in the poll books.[103]

The following sections describe these missing or inadequate features and areas that can be improved.

[103] 25 P.S. § 3535 (Repeat voting at elections).

Features that were missing or inadequate within the SURE system which could reduce or prevent errors

The SURE system does not prevent applications with non-Pennsylvania residential addresses from being approved.

County election staff (staff) are able to enter a voter's "residence address" in SURE that includes zip codes and states that are outside of Pennsylvania. The SURE system provides fields for both a "residence address" which should be in Pennsylvania because residency is a requirement for voting, and a "mailing address" which may differ from the individual's residence and does not have to be within Pennsylvania (e.g., address for a Pennsylvania student attending an out-of-state college). The SURE system does not issue a warning message that would prompt staff to review and either reject the application or correct the inaccuracy.

As part of our data analysis, we found that of the 8,567,700 eligible voters as of October 9, 2018, the residence address in SURE for 27 voters' records contained a state other than Pennsylvania, and in some cases a zip code outside of Pennsylvania. Using auditor judgement we further researched 13 of the 27 voters using Google Maps and found that for nine of 13 records, the streets, cities, and zip codes in the residence addresses of these records appeared to be within Pennsylvania; however, the state was incorrectly entered as a state outside of Pennsylvania. Therefore, the voter appeared to be eligible to vote from review of the record. Two of the 13 records were entered in SURE as Taneytown, Maryland and the address in Google Maps verified that the address was in Taneytown, Maryland. Two of the 13 records were entered in SURE as Tallahassee, Florida, and the residence street address was blank. Therefore, for four of the 13 records, (two in Maryland and two in Florida) it appears that the voters should not have been eligible to vote based on the information in SURE. Implementing a data validation edit check to ensure the residence address is within Pennsylvania could prevent data entry errors and inaccurate records. It could also help to prevent applications for ineligible voters from being approved.

The SURE system lacks geographical mapping assistance which would reduce inefficiencies and potential inaccuracies by preventing applications from being sent to the wrong county for processing.

According to DOS and county management, the SURE system does not have the capability to utilize a geographic information system (GIS) which provides mapping assistance. The GIS could be used to identify and verify information such as the county of residence, based on the zip code entered by the applicant. This technology could prevent applications from being sent to the wrong county for processing.

During our visits to seven counties, we were informed that if an applicant lists an incorrect county when electronically completing an application or when utilizing the voter registration services offered at PennDOT's photo license centers, the application will be sent to the wrong

county for processing. Once a county receives an application (either electronically or on paper) from an individual that does not reside in that county, staff may need to conduct research in order to forward the application on to the correct county. This process is inefficient and potentially delays the processing of the application.

The SURE system lacks a "Read Only" feature for voter information that should not be edited without additional supervisory review and approval.

It may be necessary at times to edit information in a voter's record, such as a change of address or last name. There is certain personal information, however, that generally does not change, such as DOB, DL number, and Social Security number (SSN). Therefore, the information included in those fields should be made "Read Only" in the SURE system, with the ability to edit such information reserved for a higher level and only after careful review. This should be coupled with proper documentation of who made the change and why.

Currently all fields, including DOB, DL number, or SSN in SURE can be edited by county staff. DOS management and Help Desk staff stated that Help Desk staff also have the ability to make changes to a county's voter records once the county electronically gives permission and provides the Help Desk staff with access for remote control of their computer. Based on our data analysis, we found instances where it appears that DOBs had been changed to a date after the registration date. For example, the DOB in one voter record was changed on April 18, 2018 from July 4, 1952 to July 4, 2016. This is clearly an error. Implementation of "Read Only" fields would preclude staff from inadvertently editing information that should not change.

The SURE system does not have controls in place to ensure that voter registrations are not improperly cancelled within 90 days of an election.

Although performing list maintenance is required by law, counties may not cancel a voter's registration within 90 days of an election due to list maintenance activities.[104] A voter may cancel their own registration at any time, but a county may not take action to remove a voter from the active rolls based on list maintenance activities so close to an election. This helps to ensure that a voter has time to receive the notification of cancellation and take action to re-activate their voting registration in time to cast a ballot on Election Day.

Our data analysis, however, indicated that counties had cancelled voter registrations within 90 days of the 2016 federal election using cancellation codes which may indicate the voters registrations were cancelled in violation of the law. We found 155 voter registrations were cancelled within 90 days of the 2016 General Election using codes that either did not indicate the reason for the cancellation or indicated that it was due to list maintenance activities.

[104] National Voter Registration Act (NVRA), 52 U.S.C. § 20507(c)(2)(A), and the Pennsylvania voter registration law (Act 3 of 2002), 25 Pa.C.S. § 1901(b)(4).

While the number of voter registrations potentially cancelled inappropriately within 90 days of the 2016 Federal General Election may appear relatively small in number, these voters' names would not have appeared in the poll book at their precinct. Therefore, if these voters had tried to vote in that election, they would have been required to vote on a provisional ballot, which takes more time for a county to process.[105] Further, voting via provisional ballot takes more of the voter's time at the polls. Voters who are rushed to vote before work or during their lunch hour may not wait to complete the provisional voting process.

Based on the results of this data analysis, we have concluded that the SURE system does not have safeguards that would prevent counties from inappropriately cancelling voter registrations within 90 days of an election. If the SURE system included hard stops to prevent county staff from cancelling voter registrations using unallowable codes or without entering a code within 90 days of an election, DOS and counties would have more assurance that cancellations made within the restricted period were for valid reasons and not in violation of the law.

Two areas of improvement related to the PennDOT Motor Voter process and the reporting capabilities within the SURE system

Some individuals confuse the change of address prompt at PennDOT's photo license centers with registering to vote.

During interviews and in response to our survey, county election officials informed us of an issue that occurs when an individual is utilizing the change of address services at PennDOT photo license centers. The scenario described is that one of the questions asked during the process is whether the individual would like to update their address for purposes of voter registration. Officials stated that some individuals believe that by completing this portion of the process, they are registering to vote; however, this is not the case. When the change of address information is received by the county, the county searches in SURE for the individual. If they are not currently registered, the change of address information will be declined; however, there is no denial notice generated and sent to the individual that requested the change of address.

County staff are unable to process the information as a new application because not all of the necessary information has been obtained from the individual (e.g., party selection and signature to affirm that the individual is eligible to register to vote). Since the individual is not notified that their request could not be processed because there was no existing record, they may believe that they registered to vote through this action at the PennDOT photo license center. This confusion could be avoided if the individual was notified that their information was declined or if the process at PennDOT's photo license centers was changed to include all the information required to register to vote.

[105] A provisional ballot is used to record a vote when there is a question regarding a voter's eligibility. Within seven days after the election, the County Board of Elections examines provisional ballots to determine if they are valid.

The ability to create reports in the SURE system is too limited and it lacks editable report capabilities.

Both DOS management and Help Desk staff indicated that the way the SURE system is designed, the reports that DOS and counties can run are limited and some of the reports cannot be customized to provide certain detail that would be useful.

Although DOS and counties are limited in their ability to run reports, there are various reports that the Help Desk staff has the ability to run for them regarding areas such as data analysis (e.g., the number of applications processed during a certain time period for a specific county or counties) and voter record list maintenance.

As DOS seeks to obtain a replacement for the SURE system, it is recommended that the new system provide the ability for both DOS and the counties to customize and run reports regarding SURE data directly from the new SURE system themselves rather than having to request the Help Desk to prepare the reports for them. In doing so, the counties could better analyze and review records internally to improve on the accuracy of the records maintained.

Recommendations for Finding 5

We recommend that DOS:

1. Incorporate the following information technology enhancements into its design of the replacement SURE system and consider the feasibility of making some or all of these enhancements into the current SURE system:

    a. A Geographic Information System (GIS) feature and related enhancements that would check addresses to ensure the address is within the county identified on the application. This would help to ensure that electronic applications are forwarded to the correct county for processing and in the case of paper applications, county staff are immediately alerted if the address they are posting to SURE is not within the county listed on the application.

    b. An edit check that would alert or prevent county staff from approving applications that have non-Pennsylvania states and/or zip codes within their residential addresses.

    c. A “Read Only” feature for certain data fields that should not change, such as DOB, DL number, and SSN to prevent unintended edits, but enable these “Read Only” fields to be edited by designated management staff along with documenting the reason for the edit.

d. A hard-stop feature in the SURE system that would prevent county staff from cancelling voter records using unallowable codes within 90 days of an election.

e. A declination notice to be automatically generated and mailed to individuals that are not currently registered to vote but submit a change of address request for their voter registration record. This will assist in notifying those individuals that they are not registered to vote.

f. The ability for DOS and county staff to build and run their own reports, rather than having to obtain reports from the Help Desk.

2. Forward information for the four voting records that contained non-Pennsylvania residential information to the applicable counties for follow up and possible cancellation.

3. Forward information for the 23 voting records that appeared to contain inaccurate non-Pennsylvania residential data to the specific counties to research and/or correct the state name or zip code within SURE.

4. Formally remind counties of the need to properly code transactions when they cancel voter registrations as a result of list maintenance in order to reduce the number of cancellations with no reason code or incorrect reason codes.

5. Consider working with PennDOT to revise the Motor Voter process so that all required voter registration information is obtained when an individual (who may incorrectly believe they are registered to vote) requests to update their voter registration address. This will ensure that a complete application is transmitted to the respective county for further processing.

Finding 6 – A combination of a lack of cooperation by certain county election offices and PennDOT, as well as source documents not being available for seventy percent of our test sample, resulted in our inability to form any conclusions as to the accuracy of the entire population of voter records maintained in the SURE system.

One objective of this audit was to assess whether the voter records maintained within the Statewide Uniform Registry of Electors (SURE) system are accurate. Before we focus on this specific objective, we note that we have already identified the following in other findings of this report:

- Several weaknesses in Pennsylvania's voter registration process. (See *Finding 4*)
- Thousands of potential duplicate and inaccurate voter records based on our data analysis. (See *Finding 2*)

Those results do not allow us to project accuracy over the entire population of voter records. Therefore, as part of our audit procedures, we selected a random statistical sample of 196 voters from the total population of 8,567,700 voters registered in SURE as of October 9, 2018.[106] Our intent was to review source documents to confirm the accuracy of the information maintained in the 196 voter records and thus conclude as to the accuracy of the entire voter population. We could not however, verify the accuracy for 138 of the 196 records selected (or 70 percent) because source documents were either not available or were not provided as further described in detail below. Source documents include the signed voter registration applications (applications) or other documents provided by the individuals to update their voter record, such as a signed affidavit completed by an inactive voter at the polling place or a returned National Change Of Address (NCOA) mailing from the voter.[107] Specifically, we planned to verify the accuracy of the following SURE system data fields by comparing the information to source documents:

---

[106] Statistical sampling means to select a limited number of items from the population on a systematic or random basis, review/test those items, and then draw a conclusion about the entire population based on the results of the items selected for testing with a statistically measurable degree of confidence considering the accepted percent rate of tolerable error. See the *AICPA Audit and Accounting Guide* "Audit Sampling" for additional details. Our statistical sample of 196 voters was determined based on a confidence level of 98 percent and a tolerable error rate of 2 percent.
For the purpose of this audit, a "voter" is a person who is registered to vote in Pennsylvania. It does not indicate that the person has voted in an election.

[107] A person applying to register to vote is required to affirm that they are: (1) a citizen of the United States; (2) a resident of Pennsylvania and the election district in which they want to register for at least 30 days prior to the next elections; and (3) at least 18 years of age on or before the next election. When a person signs their application, they are affirming their eligibility, which includes citizenship. We did not however test citizenship because citizenship information is not maintained in the SURE system. See <https://www.pavoterservices.pa.gov/Pages/VoterRegistrationApplication.aspx>.
When a U.S. citizen submits a change-of-address form to the post office, their new address is recorded in the NCOA database. <https://www.edq.com/glossary/ncoa/> (accessed August 6, 2019). For voter registration purposes,

- Full name (first, last, and middle name or initial, if included)
- Address
- Date of Birth (DOB)
- Last four digits of the Social Security number (SSN) (if included)
- Last four digits of the Pennsylvania driver's license (DL) number or Pennsylvania identification (ID) number (if included)
- Date registered
- Party affiliation

We also planned to verify that each record had a signature image in the SURE system.

Sample selection and results.

There are three methods in which an individual can complete an application:

(1) By manually completing a paper copy of the application and it being sent to a county election office.
(2) Through the Motor Voter process which is part of the DL/ID renewal process at the Pennsylvania Department of Transportation (PennDOT).[108]
(3) Through an online application made available by the Pennsylvania Department of State (DOS).[109]

Pennsylvania (through the individual counties) conducts an annual NCOA mailing using data obtained from the Electronic Registration Information Center (ERIC) to attempt to update the information in SURE by reaching out to voters who may have moved.

[108] The Motor Voter system is the system used by PennDOT to allow a PennDOT customer the opportunity to register to vote, or to update their voter registration at the same time as they have their picture taken for their DL or ID. The Motor Voter system communicates with SURE to transmit the voter registration information from PennDOT to DOS to be parsed out to the counties.

[109] The online method includes those voters that registered either through the application available on DOS' website currently available at <https://www.pavoterservices.pa.gov/pages/VoterRegistrationApplication.aspx> or those that registered through a state agency with online services available to them. See *Appendix C* for a list of agencies through which a person can register to vote.

The following table summarizes the sample of 196 voter records and related test results:

Voter Record Test Results				
Method of Application Source	**Number of Voter Records in our Sample**	**Number of Voter Records Tested**	**Number of Voter Records that Could not be Tested**	**Reason why the Voter Records Could not be Tested**
Paper Application	84	58	26	Inadequate record retention guidance. Four counties did not respond to our request for source documents.
Motor Voter	93	0	93	PennDOT would not provide Motor Voter source documents.
Online Application	19	0	19	DOS does not maintain source documents.
Total	**196**	**58**	**138**	

Additionally, we verified that the voter record in SURE included a signature for all 196 voter records in our sample.

With regard to the table above, for the 58 voter records (30 percent) we tested, we found that the information within each of the data fields matched information contained in the source document. Therefore, we have concluded that these 58 records are accurate. Additionally, for the 138 voter records (70 percent) not tested, we could not compare the information within the data fields for these records to source documents because source documents were either not available or were not provided. As a result, we could not reach a conclusion as to whether these 138 voter records were accurate. Because of this, we could not conclude on our statistical sample, and therefore could not project our results and ultimately conclude on the overall accuracy of the voter record information maintained in the SURE system.

The remainder of this finding discusses the reasons why the 138 voter records could not be tested.

DOS has not provided adequate record retention guidance to the counties.

As noted in the above table, we could not test 26 of the 84 paper applications included in our sample. Of those 26 paper applications, 14 could not be tested because 12 counties acknowledged that they were unable to locate the source documents needed to test each record for accuracy. Further, although the SURE system has the capability of retaining scanned document images, we verified that these 14 paper applications were not scanned and attached to the respective voter record.

We analyzed the registration dates listed in SURE for these 14 paper applications and noted the following:

- Three voters registered between 2004 and 2018 (after the implementation of the SURE system)
- Eleven voters registered between 1959 and 2000 (before the implementation of the SURE system)

Based on the range of registration dates, for the auditors or other external parties to verify the accuracy of voter records for these 14 voters, the source documents (applications) would have had to be maintained by the counties for up to 60 years. In reality, the time period could be longer than 60 years for voters registering prior to the 1959 date noted in the above bullet, given that a person may not need to change voter information after initially registering.
With this information in mind, we wanted to determine the following:

1. How long does each county keep source documents, if at all?
2. What record retention guidance exists?

How long does each county keep source documents, if at all?

As part of our county survey and county visits, we asked counties two related questions. The first question was whether the county currently scans and saves the full voter registration application and attaches it to the voter's electronic record in SURE.[110] Of the 65 counties that responded, 50 replied that they scan and retain an electronic copy of the application, and 15 responded that they do not scan and retain the application.

The second related question in the survey asked whether the counties retained the hard copy applications, regardless of whether or not they scanned the documents into SURE. Of the 65 counties that responded, 58 stated they do retain the hard copy applications; however, their responses varied greatly as to their retention period including:

- Length of time required by law.
- Two years.
- As long as the voter is active/registered.
- Five years after the voter's record is cancelled.
- Indefinitely/lifetime/until the voter moves or dies.

[110] Surveys were sent to all 67 counties, including the seven counties that we visited in person and in which we conducted interviews which included the questions on the survey. Five counties did not respond to the survey; however, three of those five counties were offices that we visited. For reporting purposes, we will report in total the responses received from county staff in both the survey and during county visits. It is also important to note that the surveys were completed by the then-current county election office manager/director who may or may not have been in that position since the implementation of the SURE system.

The counties' answers to the survey relate to how the counties retain applications at the time of the survey. These answers do not necessarily reflect how the counties had been retaining applications since the inception of the SURE system nor how the counties had been keeping records for the past 60 years or longer. They are a momentary snapshot of retention practices but do not establish any longstanding policies or protocols, certainly nothing that would constitute uniformity across the Commonwealth. As a result, we found during our testing that although many of the counties indicated in the survey that they scan applications, certain counties could not provide some of the applications, which may be due to the record retention policies of the counties or a difference in policy from the current election director to the former directors in the same county.

What record retention guidance exists?

Based on the results of the survey, it appears that DOS has not adequately or clearly advised the counties regarding requirements for the method of retaining applications or how long applications should be retained. DOS does not require counties to scan and attach the application to the voter record even though the SURE system has that capability. Failure to require scanning and retaining of applications causes significant non-uniformity among counties as seen by the survey results above.

As a result of the varied responses from the counties, we inquired with DOS as to what record retention policy counties must follow as it relates to the retention of applications. The policy provided to us by DOS notes that an application "must be retained for ***22 months*** from the date of any general, special, or primary election for federal office."[111] It does not, however, clarify whether the application must be retained in hard copy or if a scanned image attached to the voter's record in SURE is considered in compliance with the retention policy.

Additionally, this retention policy is not consistent with the SURE regulations establishing the SURE system which provides that: "[a] commission shall maintain the records that a commission attached to a registrant's record in accordance with § 183.4(c)(1) (relating to uniform procedures for the commissions relating to entering data into the SURE system) for 90 days after the registrant votes in any primary or election."[112] Therefore, counties are to maintain all applications received for ***90 days*** after any primary or election. These regulations have not been updated since they were initially promulgated in 2002.

Neither the *County Records Manual* nor the SURE regulations (which are different and inconsistent) provide counties record retention guidance that would allow an auditor or other external party to independently assess the accuracy of the voter registration records maintained

[111] *County Records Manual* issued by the Pennsylvania Historical and Museum Commission <https://www.phmc.pa.gov/Archives/Records-Management/Documents/RM-2002-County-Records-Manual-2017-Update.pdf> ELECTION – 1 (listed as having been last updated on **9/2012**) (accessed April 30, 2019). Please note that this manual has inconsistent revision dates within the document.
[112] 4 Pa. Code § 183.12(d)(1).

in SURE. Further, based on the counties' responses, it appears that the counties may not be aware of the retention policy in the *County Records Manual* nor the SURE regulations. As a result, it appears that county election officials determine the record retention policy. The problem is further compounded during turnover of county election officials.

A clear record retention policy from DOS and a requirement to scan all applications into SURE would help to ensure uniformity among all counties, ensure complete records, provide a SURE user with the ability to answer questions if/when they arise from either voters or county staff, and allow for documents to be audited, as necessary.

Four counties did not respond to our requests for source documents.

As noted in the above table, we could not test 26 of the 84 paper applications (over thirty percent) included in our sample. Of those 26 paper applications, 12 could not be tested because these documents were not scanned and retained in SURE, nor did the respective counties respond to our requests to provide us the 12 source documents. Overall, we requested these documents at least three times through DOS, but the counties never responded. These four counties were Allegheny, Bucks, Warren, and York.

By failing to respond, we do not know whether or not these counties actually possess the documents in paper copy. As noted above, inadequate record retention guidance may have been a factor. Therefore, the inability to review the documents impeded our ability to complete the audit objective resulting in a scope limitation. See *Finding 1* for further information. Not responding, however, gives the appearance that these counties were not cooperative with the auditors.

PennDOT refused to provide access to Motor Voter source documents.

On December 10, 2018, we requested through DOS that PennDOT provide us with access to review records for our selected sample of voters that support the voter registration information submitted by voters through Motor Voter. Specifically, we wanted to confirm the accuracy of the information maintained in SURE to the voter registration information collected by PennDOT and transferred to DOS. To accomplish this, we requested that PennDOT staff permit us to review with them (in an "over the shoulder" observation) the Motor Voter information for our selected sample records on their system. This method would ensure that our review of any documents deemed sensitive would be done in the presence of a PennDOT employee. This is a common practice that is applied to numerous audits and is generally well-accepted. Utilizing this supervised method of review would avoid the possibility of the auditors inadvertently obtaining documents containing personally identifiable information from PennDOT. In fact, it was consistently communicated to both DOS and PennDOT that the auditors prefer not to review personally identifiable information.

As a result of this request, we met with PennDOT management and legal counsel on January 7, 2019, to explain our request and to answer any questions they had. We also explained that failing to provide the information would preclude us from being able to conclude on the accuracy of the voter registration records in SURE. PennDOT indicated that the information we were requesting to see was not easily retrievable and the timing of it was not good due to their REAL ID Act program which would be starting in March 2019. PennDOT indicated however, that they would consider our request.[113]

We sent requests for this and additional information ***a total of seven times***; however, we did not receive any information from PennDOT until April 17, 2019, which was after our audit procedures closing date of April 16, 2019. In lieu of allowing us to perform the "over the shoulder" procedure, PennDOT provided us with limited documentation, but this did not contain all the Motor Voter information we needed to complete our accuracy test. Therefore, we were unable to verify the accuracy of the voter record information in SURE that was received via the Motor Voter system. The failure to fully cooperate is considered a scope limitation and significantly affected the auditors' ability to reach conclusions on the stated objective, which in turn minimized the overall value of the original objectives agreed upon by DOS. Despite these limitations, we sought to present at least some meaningful conclusions to the public. See *Finding 1* for further information.

DOS does not maintain online application source documents.

We were unable to review voter registration support documents for any of the online applications in our sample. DOS management acknowledged that there is no source document created for online applications. The SURE system is not designed to maintain a record of the original electronic information forwarded to the county election offices in batches for processing, nor are county election staff required to maintain documentation supporting the electronic information they receive. If county election staff were required to print out the information received online, scan it into SURE, and then save it to the voter's record, a source document would be available for review if needed. Although this would require extra steps by the county election staff, it would provide access to source documents and allow for the auditability of the data.

[113] The REAL ID Act, effective May 11, 2005, establishes specific minimum federal standards for state-issued driver's licenses and ID cards to be accepted for certain federal purposes, like entering a federal building or boarding a domestic commercial flight. Enforcement of the REAL ID Act begins on October 1, 2020 in Pennsylvania. https://www.dmv.pa.gov/Pages/REAL-ID-Frequently-Asked-Questions.aspx (accessed August 6, 2019).

Recommendations for Finding 6

We recommend that DOS:

1. Develop an effective audit trail for registration applications received online to enable either DOS or county election staff to review and confirm the accuracy of information in SURE to the original point of entry of information by the registrant. If this cannot be accomplished through electronic means, see Recommendation 2.

2. If DOS is unable to electronically implement Recommendation 1, it should develop a policy requiring county election staff to print out and scan into SURE voter registration related documents that are received online and attach the documents to the voter's record.

3. Develop a policy requiring the counties to scan all voter registration related documents that are received via hard copy to the voter's record. This will allow for access to the original documents that support information entered into a voter's record in SURE and to help ensure uniformity amongst all the counties.

4. Develop and issue a directive regarding records retention for SURE and work with the Pennsylvania Historical and Museum Commission (PHMC) to confirm that its *County Records Manual* regarding election records is entirely uniform with the SURE records retention directive to help ensure consistency of records retention amongst all the counties. Consideration must be given to the availability of source documentation for purposes of evaluating accuracy of the voter registration information by an external party. The directive should be placed in a prominent location of DOS's website and should be sent at least yearly to all county election offices.

5. Update the SURE regulations to ensure that they are in accordance with the newly developed and distributed record retention policy and the updated PHMC *County Records Manual*.

Finding 7 – The Department of State should update current job aids and develop additional job aids and guidance to address issues such as duplicate voter records, records of potentially deceased voters on the voter rolls, pending applications, and records retention.

From January 2003 through December 2005, the Department of State (DOS) utilized a phased-in approach for implementing the Statewide Uniform Registry of Electors (SURE) system in all 67 counties. As a result, county election offices (counties) have been using the SURE system to process and maintain voter records for more than 15 years. Prior to that, each county maintained its own voter registration system. With the creation and implementation of SURE, there was a need to train county election staff and to provide a resource for updated and ongoing guidance. According to DOS officials, DOS provided initial training to all counties as implementation occurred.

Based on our audit procedures covering the period January 1, 2016 through April 16, 2019, we found that DOS generally provided meaningful assistance and guidance to the counties regarding SURE voter registration and list maintenance. We believe, however, that they did not sufficiently address all critical areas. Job aids should be updated and additional job aids should be developed to help improve the accuracy of voter record information. The critical areas not adequately addressed, along with the current level of guidance provided, are listed below:

- Job aids need to be updated to reflect improvements recommended for the SURE system regarding review for duplicate voter records and records of potentially deceased voters on the voter rolls.
- Length of time that voter registration applications (for new registrations or change of name, address, or party affiliation) should remain in pending status – No guidance.[114]
- Record retention policy – No clear guidance (See *Finding 6*).

The following sections describe the assistance DOS provides to the counties and the critical areas on which DOS should further develop and distribute guidance to the counties.

Hands-on training upon request.[115]

We found that although DOS does not schedule required, regular/on-going training for county staff, training is available upon request by the counties. Based on our survey results from 65 counties, 19, or approximately 30 percent, indicated that they requested hands-on training since their initial training. According to DOS management, nine counties were provided a total of 13

[114] When an application is missing a required piece of information it is placed in pending status while the county attempts to obtain the missing information from the applicant. The application, while in pending status is neither approved nor denied, and therefore the applicant is not a registered voter.
[115] Training is provided to county staff in person at DOS offices in Harrisburg.

training sessions during our audit period. Training requested by the other ten counties was provided prior to the beginning of our audit period, January 1, 2016.

Access to the SURE Help Desk.

DOS contracts with a vendor to provide assistance to counties regarding day-to-day SURE questions through a SURE Help Desk as well as training for any new SURE system processes. The Help Desk is comprised of two tiers. Tier 1 is the first point of contact for a county official calling for help. The Tier 1 Help Desk staff stated that they are trained and have access to written guidance on the SURE system to answer most questions from the counties. Tier 2 encompasses two areas: (1) operational support and (2) application development and complex/technical assistance. Tier 2 is a resource when Tier 1 staff cannot answer a county's question, as well as providing training to Tier 1 staff when system changes are scheduled. This ensures that Tier 1 staff are ready to answer any questions/concerns the counties have after deployment of the system change.

We visited seven counties as part of our audit procedures. All seven counties informed us that the Help Desk is an invaluable tool that they use regularly. The responses received from the county survey we conducted also supported this with 40 of the 62 counties that responded to the survey indicating that they contact the Help Desk on a weekly basis.

Job aids need to be updated to reflect improvements recommended for the SURE system regarding review for duplicate voter records and records of potentially deceased voters on the voter rolls.

DOS, in conjunction with Help Desk staff, creates and electronically distributes SURE job aids to the counties. Job aids are documents that are meant to provide guidance on the current processes established in the SURE system and include, among others, the following helpful features: descriptions of a particular job process; step-by-step instructions on how to perform the process in SURE; and screen shots taken from the SURE system with explanations on using the features in SURE. As described in *Finding 2, however,* there are improvements that should be made in the SURE system regarding work that should be performed by the county election office staff regarding checking for: (1) duplicate voters when processing new voter registration applications; and (2) registered voters on the Pennsylvania Department of Health death records. The recommended improvements will assist in ensuring the accuracy of the data in voter registration records. As a result, as improvements are made to the SURE system, the job aids need to be updated to reflect the processes associated with the improvements.

According to DOS management, the job aids are updated as necessary, typically preceding any enhancements to the SURE system. The job aids are emailed to the counties two days prior to an enhancement and are also posted online within SURE. If a job aid needs to be updated, the new

version is posted and the old version is removed in order to avoid confusion as to which one is the most recent.

In order to determine how helpful the counties find the job aids, our survey inquired whether the counties actually use them. The majority of counties (60 of the 65 counties that responded) confirmed that they use the job aids; however, the counties overwhelmingly noted that they find it easier and prefer to call the Help Desk with questions. This is not because the job aids are confusing, but because they find the Help Desk extremely useful.

DOS provided us with copies of the 64 job aids that were used throughout our audit period. Based on job aid topic titles, we determined, and DOS management confirmed, that 19 of the 64 job aids were applicable to our audit objectives. Our audit procedures included a review of these 19 job aids. We found them to be titled in a manner that makes it easy to determine the topic covered in the job aid, as well as being informative and easy to follow. Based on our review and knowledge of the SURE system, we are in agreement with the general responses received from the counties in both the interviews and survey responses that the job aids are adequate for use in navigating the current SURE system; however, as improvements are made to the SURE system, the job aids need to be updated accordingly.

Another area of concern that we noted was that only 62 of the 64 job aids included a date and the format of the issued date varied. Some included the full date, while others only included the month and year, or only the year in some cases. Although, according to DOS management, it removes the outdated job aids from SURE, many county election directors reported to us that they print hard copies and distribute them to their employees for quick reference. For this reason, it is imperative that DOS ensures that all job aids are dated in a uniform manner to provide a means for users to confirm that they are using the most recent and applicable job aid to assist them in performing the necessary function in SURE.

The following section provides details regarding a critical area not addressed in which an additional job aid should be developed to help improve the timeliness of processing applications that are placed in pending status.

No guidance was provided to counties regarding the length of time that applications remain in pending status and whether pending applications past that timeframe should be denied.

Voter registration applications (applications) that are missing required information or require follow-up with the applicant are placed into pending status until a determination can be made to approve or decline the application. Currently, there is no guidance from DOS to counties with regard to the following:

- The evaluation of pending applications to determine whether the applications should be approved or denied.
- The length of time that applications should remain in pending status.

DOS management indicated it was aware of the issue regarding pending applications and was reviewing its legal authority to direct counties on what actions to take to help eliminate the high number of pending applications.

As noted in *Finding 4*, our data analysis identified more than 54,000 potential applications which have been in pending status for one or more years. When an application is placed in pending status due to missing information, the applicant is sent a letter requesting the missing information. Not all applicants, however, respond to the letter and provide the missing information. When an applicant fails to respond, their application remains in pending status indefinitely.

As reported in *Finding 4*, according to the data we reviewed, 95 percent of applications in pending status are waiting for a response from the applicant. DOS management stated that it would be more beneficial to the applicant and the county if the counties rejected the pending applications for a lack of a response from the applicant after a pre-determined amount of time set by DOS. Once rejected, the counties would send a notification to the applicant. This notification could prompt the applicant to re-apply, rather than the applicant being unaware that they are not registered to vote until they arrive at a polling place on Election Day only then to discover that their name is not included in the poll book. It would also be beneficial for the counties as they would no longer have thousands of pending applications remaining stagnant in SURE for years. See *Finding 4* for more information regarding pending applications.

Recommendations for Finding 7

We recommend that DOS:

1. Continue to offer hands-on training on the SURE system and ensure that all counties are made aware of the availability of this training.

2. Update the applicable job aids as appropriate to reflect changes in processes. For example, added steps for identifying duplicate voters when processing applications or linking a Department of Health death record with a registered voter.

3. Include an issued date (month, date, and year) on all job aids distributed to the counties and an indexed list of all job aids readily available on DOS' website to provide a reference as to which version of a job aid is the most current and the date of the revision.

4. Provide guidance to the counties regarding the maximum length of time that an application can remain in Pending status and how to appropriately determine whether the application should be approved or rejected, if it is determined that DOS has the legal authority.

Agency's Response and Auditor's Conclusion

We provided copies of our draft audit findings and related recommendations to the Pennsylvania Department of State (DOS) for its review. On the pages that follow, we included DOS' response in its entirety. Following the agency's response is our auditor's conclusion.

Audit Response from the Pennsylvania Department of State

PENNSYLVANIA DEPARTMENT OF STATE

RESPONSE TO DRAFT PERFORMANCE AUDIT REPORT

I. Introduction and Background

In November 2017, the Department of State (DOS) began discussions with the Department of the Auditor General (DAG) to help DOS in our preparation to transition to a new voter registration system to replace our Statewide Uniform Registry of Electors (SURE) system. We believed that an audit would help us confirm and identify tools and improvements to seek in a new system and help support our requirements-development process for the RFP for the new system. These objectives were built into the audit.

Around the same time, DOS was contacted by a few senators who wished to discuss possible legislation regarding a SURE security audit. In December 2017, DOS staff, DAG staff and Office of Information Technology (OIT) staff attended a meeting with senate staffers. During the meeting, there was discussion about what the scope of the audit should include. Two primary factors limiting the scope of the audit that were discussed were the Commonwealth's obligation to protect critical infrastructure information under state and federal law and policy as well as pursuant to security best practices, and DAG's express acknowledgment of its lack of expertise and knowledge to conduct a substantive security audit.

The three parties worked together to design a compromise as set forth in the Interagency Agreement (IA)[1] which would limit the security portion of the audit to solely a review of the security protocols of the SURE system, *see* IA ¶ 2.a.iii., or in other words, confirm that appropriate protocols are in place to secure our voter registration system. Security experts agree that such protocols include, but are not limited to, practices such as utilization of continuous network monitoring, inventory identification, intrusion detection sensors, engaging in regular third-party vulnerability and cyber assessments, firewalls, encryption, password protection, multi-factor authentication, security awareness training, risk management, continuity of operations (COOP) planning, disaster recovery, and code reviews and scans. The parties agreed that should there be any dispute between the parties, such disputes would be submitted to the Governor's Office of General Counsel for resolution. *See* IA, ¶ 4.i.

A. Election Security in Pennsylvania

As expressed in Exhibit A, *Letter from the PA Interagency Election Security and Preparedness Workgroup to the Auditor General,* the Commonwealth takes its responsibility to protect the vote very seriously, and is proud to lead the country in using strategic partnerships with federal, state, and county officials and the private sector, to deploy election security best practices and innovative responses to the ever-changing world of cyber security threats. This leadership was underscored most recently in

[1] *See* DAG's Report, App. B for a copy of the IA.

Secretary Boockvar's appointment as the co-chair of the Elections Committee of the National Association of Secretaries of State, as well as her invitation to provide expert testimony at the bipartisan hearing "Securing America's Elections" of the Judiciary Committee of the United States House of Representatives on September 27, 2019. *See* Exhibit B*; see also* https://judiciary.house.gov/legislation/hearings/securing-america-s-elections and https://docs.house.gov/meetings/JU/JU00/20190927/110038/HHRG-116-JU00-Wstate-BoockvarK-20190927.pdf

During this audit, DOS and the Office of Information Technology (OIT) provided DAG with hundreds of pages and hours of presentations, meetings to review and discuss security protocols with "over the shoulder" access to certain information, affidavits, and materials evidencing Pennsylvania's leading information technology and other security protocols and practices to secure the SURE system and protect our elections. These materials included but were not limited to:

- A high-level overview, presented by Christopher P. Dressler, the Chief Information Security Officer for the Employment, Banking and Revenue Delivery Center,[2] of the various external security and assessment reports.
- An extensive two-hour presentation by Erik Avakian, the Chief Information Security Officer for the Commonwealth of Pennsylvania, to review the Commonwealth's cybersecurity program and posture.
- An affidavit executed by Christopher Dressler outlining the multiple mitigating security controls employed by OIT to protect the SURE system.
- Access to over 100 security and cyber hygiene assessments, redacted except for the cover page and section headings, to not only demonstrate the existence of such reports but also to corroborate the repeated information DOS provided to DAG regarding the number and frequency with which those security assessments occur.
- Dozens of SURE user manuals and job aids.
- Dozens of DOS policies, directives and memoranda.
- Access to the SURE Portal and over-the-shoulder access to SURE so that DAG staff could not only ask questions but also review records themselves.
- Access to DOS' Continuity of Operation (COOP) plan summary and scope document
- Access to DOS' high-level disaster recovery plan and table exercise

[2] The Employment, Banking and Revenue Delivery Center provides IT service to DOS as part of the shared service model for state agencies under the Governor's jurisdiction.

- A copy of the Department's policy related to identification, handling, and protection of critical election infrastructure, otherwise known as the TLP policy.

- Provided proof of patching schedules related to underlying infrastructure and architecture.

As described in the letter in Exhibit A, and documented in the above and other presentations, affidavits, and materials, the Commonwealth's strong security protocols include, but are not limited to, the following:

- We engage in 24/7 continuous network monitoring, constant contact with the Center for Internet Security's Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), inventory identification, intrusion detection sensors, infrastructure/network diagrams, regular third-party vulnerability and cyber assessments, firewalls, encryption, password protection and multi-factor authentication in access to email, file storage, systems, and other resources.

- The Commonwealth utilizes multiple layers of protection, controls, and end-user security awareness training, risk management, policy compliance assessments, continuity of operations (COOP) planning, disaster recovery, and code reviews and scans as part of a comprehensive cybersecurity program. Additionally, several DOS staff have national security clearances to extend our access to classified information that will bolster our election security.

- Pennsylvania continues to be a nationally recognized and award-winning leader among states in cybersecurity. Our extensive collaboration, including the formation of the Pennsylvania Interagency Election Security and Preparedness Workgroup in 2018, is considered a notable model that many other states are interested in replicating. In addition to DOS, OIT, and the Governor's office, our multi-layered and cross-sector partners include the U.S. and PA Department of Homeland Security, Pennsylvania Emergency Management Agency (PEMA), Pennsylvania State Police, Pennsylvania Department of Military and Veterans Affairs, Pennsylvania Inspector General, County Commissioners Association of Pennsylvania (CCAP), and Center for Internet Security (CIS), among others. We also formed a county/state election security workgroup consisting of CCAP, county election directors, DOS staff, and county and state CIOs and IT personnel.

- Beginning in the 2019 primary, our teams moved our election-day operations to PEMA headquarters. To strengthen our security and responsiveness and enhance our collaboration and coordination, the Commonwealth's election experts, security teams, call center, cybersecurity experts, law enforcement, and state emergency personnel are now able to closely monitor developments throughout the day from

one location with all of PEMA's resources close at hand. Our election, security, and preparedness professionals also participate across the state and across the country in real-time information-sharing on cyber issues, as well as on-the-ground and weather-related situations that could impact voting.

- The Commonwealth also provides anti-phishing and security training and tools to all 67 counties at no cost to them, and our state and federal partners such as the U.S. Department of Homeland Security and the Pennsylvania National Guard additionally offer vulnerability and cyber assessments to them at no cost. Furthermore, we have collaborated with all these partners on multiple tabletop exercises for counties and partners modeled after law enforcement and emergency response techniques, to train election, IT, and security personnel in incident response and preparation, simulating scenarios that could impact all aspects of voting operations.

B. Threats to PA Elections

As Secretary Boockvar testified at the bipartisan hearing "Securing America's Elections" before the Judiciary Committee of the U.S. House of Representatives,

> The issues surrounding security have made election administration more challenging and complex than ever. As we have learned over the last several years, foreign adversaries and other cyber actors have attempted and continue to attempt to influence elections in the United States. The key to thwarting this effort is that we must continue to build and strengthen our walls faster than those that are trying to tear them down. Election security is a race without a finish line, and our adversaries are continuously advancing their technologies. We must do the same and more; our success is dependent on substantial and sustained dedication of resources.

Exhibit B, p. 1. These issues and challenges are why the Commonwealth, and our Inter-agency Election Security and Preparedness Workgroup has employed such a committed, multi-layered, and cross-sector security strategy to election security in Pennsylvania.

C. Election-Related Responsibilities of DOS and County Election Offices

On pages 3 and 4 of the draft audit report, DAG briefly describes the duties of two of the bureaus within the Elections Deputate, which was divided in February 2019 into three bureaus to be better equipped to meet the evolving challenges of election security and technology and augment our civic engagement and campaign finance outreach and programs. A summary of these three bureaus are as follows:

- Bureau of Election Services and Notaries (BEN)– Jessica Mathis, Director. This bureau oversees the functions of the Division of Election Services and Voter Registration, as well as the Division of Notaries. The bureau is responsible for serving voters, candidates, counties, and other stakeholders on matters relating to election administration, voter registration, legislation, and notarial acts.

- Bureau of Election Security and Technology (BEST) – Michael Moser, Director. This bureau oversees the functions of the SURE division and election security and technology initiatives. It is responsible for working with federal, state, and local partners to maintain and enhance the security of Pennsylvania's election infrastructure. The bureau also oversees the voter registration and election management systems, certification of equipment, and technology and data innovation.

- Bureau of Campaign Finance and Civic Engagement (BCFCE) – Tiffany Chang Lawson, Director. This bureau oversees the functions of campaign finance and lobbying disclosure, and works closely with stakeholders, candidates, elected officials, and the public. The bureau also houses and leads the Governor's Civic Engagement Award program, as well as manages DOS's Language Access Plan.

D. **Implementation of SURE**

DAG correctly notes on pages 4-5 of the draft audit report the limits of DOS's authority including lack of enforcement authority regarding voter records. However, despite limits to our statutory authority, DOS facilitates the requirements of Act 2002-3, 25 Pa.C.S. §§ 1101 *et seq.*, imposed upon county voter registration commissions through SURE. The SURE system is also the first-time county legacy systems were migrated into one statewide system. In addition to the tools necessary for counties to meet their statutory duties, DOS provides services through SURE and the SURE Portals to counties and voters that are not explicitly mandated by either federal or state law. For example, DOS provides convenient online tools to voters, which enable them to confirm their registration information online and submit an online application if their information needs to be updated. These tools are also an efficiency to county election personnel.

E. **Commonwealth's Voter Registration Process**

DAG's overview in Appendix C (pp. 77-80) summarizes the voter registration process in Pennsylvania. And while DAG correctly cites to court challenges in states that have enacted documentary proof of citizenship, the U.S. Supreme Court has held that the National Voter Registration Act ("NVRA") forbids states from demanding that applicants submit additional information beyond that required by the federal form—striking down

an Arizona law requiring documentary proof of citizenship from people seeking to register using the federal voter registration form. *See Arizona v. Inter Tribal Council of Arizona, Inc.*, 570 U.S 1 (2013).

Additionally, in Appendix D, regarding the issue with the PennDOT motor-voter system that had allowed ineligible individuals to inadvertently register to vote, it is important to note that DOS acted expeditiously as soon as it became aware of the issue. To be clear, the issue spanned several decades and multiple administrations. DOS became aware of the issue in late summer 2017, and the resolution to fix the problem and prevent future occurrences, which necessitated a change to PennDOT's computerized motor-voter procedures, was completed by early December 2017.

Importantly, DOS informed DAG that the expert data analysis requested by DAG is protected by the attorney-client privilege and the attorney work product doctrine and are not subject to disclosure. DOS remains involved in litigation brought by a third party seeking to access this very same privileged information (as DAG is aware, *see* DAG's Report, App. D, n. 130). Disclosure of the privileged analysis to the DAG would have immediate waiver consequences.

Finally, in response to DAG's recommendation that DOS and the counties must continue to address this concern, DOS states unequivocally that we take very seriously the charge to make sure only eligible voters can cast ballots. We have shared the necessary information with the counties, who are authorized to take further action to confirm eligibility and remove ineligible voters as appropriate.

F. Voter Record Maintenance Process

DOS provides counties with multiple tools for maintaining the accuracy of their voter records and conducting list maintenance, including the National Change of Address (NCOA) program, the Electronic Registration Information Center (ERIC) program, and the 5-Year Notice program.

DOS works together with the members of the SURE Advisory Board created by section 1302-C of the Election Code, 25 P.S. § 3150.2, to periodically update the tools and guidance relied upon by the counties to conduct voter list maintenance, including voter correspondence, list maintenance reports, and job aids.

G. Status of Pennsylvania's Voting Systems

The topic of Pennsylvania's Voting Systems falls completely outside the scope of DAG's audit parameters; there is nothing even remotely applicable to voting systems in the Interagency Agreement. Nonetheless, we welcome the opportunity to recount the significant progress Pennsylvania counties are making in transitioning to new voting systems with auditable paper trails.

First, we want to correct several errors in DAG's summary in this section. One, not all PA counties lacked a paper record in April 2018; 50 counties did. Two, Pennsylvania has already received $14.15 million – this occurred in August 2018. Of these funds, 95% were received from the federal government, plus a 5% state match. More than half of the counties have already begun or have completed the process of receiving their share of the funds. Three, in most counties, the federal dollars amount to at least 10-12% percent of the county cost for the new systems.

The counties are very dedicated to upgrading their voting equipment and worked hard over the last year to meet the upcoming deadline. Last spring DOS directed the counties to select new voting systems meeting current security and accessibility standards with voter-verifiable paper trails by December 31, 2019 and implement them by the 2020 primary. All these new systems were subject to penetration testing, access control testing to confirm detection and prevention of unauthorized access, and evaluation that every physical access point is well secured and system software and firmware is protected from tampering.

To date, at least 53 of 67 counties - 79 percent of Pennsylvania's counties- have voted to select new voting systems which meet current security and accessibility standards with voter-verifiable and auditable paper trails, whereas a year ago, 50 out of 67 counties used paperless DRE voting machines. Remarkably, this November 51 out of 67 counties will be voting on systems with auditable paper records.

Additionally, in January 2019, DOS formed a post-election audit workgroup, which since that time has been studying models of post-election audits. The members of the workgroup include:

- Allegheny County Election Director David Voye
- Lancaster County Election Director Randall Wenger
- Mercer County Election Director Jeff Greenburg
- Mifflin County Election Director Zane Swanger
- Philadelphia Deputy City Commissioner Nick Custodio
- Sullivan County Election Director Hope Verelst
- Brennan Center Democracy Program Counsel Liz Howard
- Common Cause PA Executive Director Micah Sims
- Verified Voting Senior Science and Technology Policy Officer Mark Lindeman
- Department of State representatives:
    - Acting Secretary of State Kathy Boockvar
    - Deputy Secretary for Elections & Commissions Jonathan Marks
    - Director of Election Security and Technology Mike Moser
    - Director of Policy Jessica Myers
    - Director of Elections and Notary Services Jessica Mathis
    - Voting Systems Analyst Sindhu Ramachandran

The workgroup will develop recommendations by January 2020, will work with the legislature for any suggested legislative enhancements, and will carry out pilot audits in multiple counties across the Commonwealth in 2019-2021. By November 2022, all counties will utilize the new enhanced audits.

The first audit pilots in PA will occur in November 2019 in Mercer County and Philadelphia. We will be partnering with local election officials and respected experts to audit both the plain text on the paper records and the tabulated votes to confirm the outcome of the election. The feedback from these pilots will enable the Department of State, in conjunction with local election officials, to establish and test real-time best practices.

Expert partners for the pilot audits include the U.S. Election Assistance Commission, University of Michigan, VotingWorks, Democracy Fund, Verified Voting; Common Cause Pennsylvania, and the Brennan Center for Justice at NYU School of Law.

These audits are scientifically designed and utilize highly effective procedures conducted after an election to strengthen election security and integrity, confirm the accuracy of election outcomes, and provide confidence to voters that their votes are being counted accurately.

In July 2019, Governor Wolf announced that the Commonwealth would begin work to issue a bond to assist counties with purchasing new voting systems with a paper trail. Under the arrangement, the Commonwealth would fund up to $90 million to reimburse counties for approximately 60 percent of their actual costs to replace voting systems, on top of the 10-12 percent they are already receiving from the 2018 federal appropriation.

On October 31st, Governor Wolf signed historic bipartisan election reform, Act 2019-77, that included authorization for the $90 million in bond funding to aid counties with the purchase of new voting systems with a paper trail. The Pennsylvania Economic Development Financing Authority (PEDFA) is preparing to issue this bond following a board vote, and the Department of State will make grants available to counties once established.

H. DOS Plans to Replace the SURE System

DOS worked with federal, state, and county partners for more than a year to finalize the RFP for a new voter registration and election administration system to replace the current SURE system. The RFP was posted for vendor solicitation on October 9, 2019. Responses to the RFP are due in late November 2019, and the selection committee, which includes program and security experts in addition to county election personnel, will begin review and scoring after that time, with selection and approvals to be issued in 2020. The new system goes live by the end of 2021, after extensive transition, training, and careful implementation statewide.

II. **Finding 1** – As a result of the Department of State's denial of access to critical documents and excessive redaction of documentation, the Department of the Auditor General was severely restricted from meeting its audit objectives in an audit which the Department of State itself had requested.

DOS strongly refutes Finding 1 and stands firmly behind its decision to maintain the confidentiality of the Commonwealth's critical infrastructure information. As stated by the *Pennsylvania Interagency Election Security and Preparedness Workgroup*, composed of the Pennsylvania Office of Homeland Security, Pennsylvania Emergency Management Agency, Pennsylvania State Police, Pennsylvania Department of Military and Veterans Affairs, the Pennsylvania Inspector General, DOS, and OIT,

> As security and preparedness experts, we fully concur with the Department of State's and Office of Information Technology's protection of these documents and determination that they could provide only redacted copies of this information to [DAG]. **We believe their actions embody and uphold the highest standards of security protocol for the Commonwealth.**

Exhibit A, *Letter from the PA Interagency Election Security and Preparedness Workgroup to the Auditor General.*

Alleged Scope Limitation A

The Commonwealth has for quite some time protected documents and other information related to sensitive security matters. In January 2017, the Federal Department of Homeland Security (DHS) designated election infrastructure (EI) as critical infrastructure information (CII) under the "Government Facilities" sector, which generated even stronger protection at all levels, to further strengthen our nation's security.

These significant protocols governing protection of information relating to election security were discussed with DAG from the very early communications before the audit even began and continued throughout the audit. As stated on page 1 of this response, DAG's objective relating to election security was solely to confirm that appropriate protocols were in place to secure our voter registration database. At no point did DOS or OIT ask DAG to evaluate the security assessments, system configuration, action plans, nor any other protected critical infrastructure information. In fact, DAG had explicitly informed DOS that they had nobody on staff who had expertise in evaluating this type of information and they were happy to note that we were working with DHS and OA-OIT, as well as experts at other state and federal agencies.

Rather, DAG was provided with briefings and documentation, albeit redacted to protect critical infrastructure and cybersecurity information, about the components of the internal controls that were and are in place for the election system. This information included an explanation of the use by the Commonwealth of security experts such as the Department of Homeland Security and other expert security advisors, to regularly assess our internal controls and security and make

recommendations to continue to build and strengthen our protections. We follow best practices and are continually advancing these protocols, and we provided DAG with hundreds of pages and hours of presentations, affidavits, and materials evidencing Pennsylvania's leading information technology and security protocols and practices to secure the SURE system and protect the integrity of our elections and voters.

As stated in Exhibit A, *Letter from the PA Interagency Election Security and Preparedness Workgroup to the Auditor General,*

> Protection of critical infrastructure information is and has been one of the essential security protocols recommended by security experts at every level.... As security and preparedness professionals, we cannot emphasize enough how important this protection is in order to carry out our duty and responsibility to the citizens of our Commonwealth. This means that information such as vulnerability and cyber assessments, system configuration and architecture, disaster recovery plans, and other types of information that relate to our critical infrastructure should under no circumstances be shared with anyone other than those with an absolute need to know in order to perform homeland security duties.

As we informed DAG repeatedly, this protection is supported by exceptions in the Pennsylvania Right to Know Law and the federal Freedom of Information Act, as well as protection under the Commonwealth Information Technology Policy ITP-SEC019, the Cybersecurity Information Sharing Act of 2015, the Protected Critical Infrastructure Information (PCII) program, and the federal and DOS's Traffic Light Protocol (TLP) policy.

In addition, the U.S. Department of Homeland Security (DHS) and Pennsylvania have specifically identified for PCII protection and TLP Red designation critical infrastructure documents including, but not limited to, system assessments, phishing campaigns, risk and vulnerability assessments, vulnerability scanning (cyber hygiene), architecture review, and cybersecurity evaluation tools.

To foster cooperation and help meet the audit objectives, DOS and OA/OIT offered to provide extensive presentations regarding the cybersecurity assessments, controls and frameworks utilized by the Commonwealth, as well as hundreds of pages of redacted assessments in lieu of the protected documents. As a result, in addition to numerous meetings over the course of the audit process, there were at least two key presentations by OIT's security leadership to DAG, one in October 2018, and one in April 2019.

In the October meeting, DOS met with the DAG team in person to review and discuss high-level overviews of the multiple external security assessment and vulnerability reports we have received for years from DHS and other third-party experts. During the meeting, DOS and DAG reviewed a blank sample of the DHS reports indicating the scope of examinations and testing performed as part of the third-party assessments, so DAG could have an understanding of what was included in these evaluations and reports.

In the April presentation, the DAG team was provided with an in-person presentation by OIT giving a comprehensive overview of the Commonwealth's multi-layered cybersecurity approach

and strategy, collaboration between federal, state and local partners, and assessments performed in our technical environment. In addition, the presentation demonstrated that the Commonwealth's IT controls follow the guidance of the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and industry best practices. In fact, the presentation covered all five core categories of the NIST CSF (Identify, Protect, Detect, Respond and Recover), and reviewed with the DAG team the various measures, processes and procedures in place within each category.

Furthermore, the DAG team was provided with in-person meetings by DOS giving a comprehensive overview of the user provisioning, privileged user and system administrator roles and access in March and April. While some of the follow-up documentation was redacted to protect copies of sensitive information, the DAG team was afforded the opportunity to see a display, or "over the shoulder" access, of the credentialing process in production as well as privileged user access and responsibilities.

As evidenced in hundreds of pages and hours of presentations, affidavits, and materials shown to DAG, DOS and OIT demonstrated their extensive utilization of leading information technology and other security protocols and controls. Furthermore, they did so in a manner that not only meets best practices and requirements of IT General Controls and other standards, but also embody and uphold the highest standards of security protocol and protection of critical infrastructure information for the Commonwealth.

We were very pleased on Election Day to welcome Chris Krebs, Director of the U.S. Dept of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA). CISA's election security team has been an instrumental partner in securing our elections in Pennsylvania and across the nation, and Director Krebs emphasized both the strength of our election security protocols and our partnerships.

In our joint press release, Director Krebs recognized Pennsylvania for its election security strengths, and noted:

"Election security is a top priority for CISA. Americans should have confidence that they are the ones picking their leaders and deciding elections without concern about foreign interference. Acting Secretary Boockvar and her team have been strong partners in this effort and continue to lead with their move to auditable systems and investment in election systems," Krebs said. "Voters have a role to play too. We know that foreign adversaries seek to influence public sentiment and may seek to spread wrong information during the election. I encourage everyone to ignore the noise and get election information straight from the source—from the Secretary of State's office or their local election office. Armed with this knowledge, Pennsylvanians can go to the polls today with confidence that their vote will be counted as cast."

Following his visit, Director Krebs tweeted "Just wrapped a visit to Harrisburg, PA, where I toured their election day operations, which includes the Pennsylvania Department of State, PEMA and the PA National Guard, all working together throughout the day." . . . "Pennsylvania has an impressive operation and has been a strong partner of the Cybersecurity and Infrastructure Security Agency."

Alleged Scope Limitation B

DAG selected a sample of 196 voter records from 8.5 million plus voters that were registered as of October 9, 2018 and requested live "over the shoulder" access to view screens containing an actual image of each individual driver's license. As was explained to DAG in February 2019, PennDOT does not maintain an actual image of driver's licenses; rather the information used to create a driver's license is stored across several databases and systems.

As a result of this limitation and the inability to provide the requested "over the shoulder" access a compromise was reached whereby DAG on February 14, 2019 requested "screen capture printouts of the original screens from PennDOT's computer files." To gather the requested information, PennDOT requested identifying information for the 196 selected records.

Prior to providing responsive information a Non-disclosure Agreement (NDA) was required between DAG, PennDOT and DOS. The NDA was executed on April 16, 2019 and on that same day responsive information was provided to DAG. PennDOT provided DAG with two cumulative records: one that contained a file export in the form of an excel spreadsheet that contained PennDOT customers whose driver's license was processed after the implantation of DDL (67 records); the other a PDF that contained screen shots of customer records that were processed prior to the implementation of DDL (120 records). PennDOT was not able to provide verification information for six of the requested records as additional information was required for five of the records and one of the records was inactive.

DAG is inaccurate in their statement that DOS does not maintain source documentation for Online Voter Registration applications and Motor Voter applications. DOS maintains source data for both Motor Voter applications and Online Voter Registration applications. This data is stored and never altered even after the applications are sent to county officials for review. This data is housed in multiple locations within the SURE architecture.

Though DOS does not have direct access to PennDOT's database or the original source data for the licensing transactions, we maintain copies of all Motor Voter application data received from PennDOT. This data can be used to audit the DOT applications that are queued in SURE for the counties to process.

With regard to the delay in responding to certain DAG requests for information, DOS agrees that many of its responses were provided beyond the third day after the DAG's requests. However, it is important to note that many of the DAG's requests for information, particularly IT requests, required the compilation of data, data schema, architectural documentation, etc. in non-native formats. Many of the requests for information also required substantial redaction by DOS staff, in consultation with counsel, to avoid unnecessary disclosure of sensitive information. Additionally, despite DAG having asked us to identify for them critical date periods which would be difficult times for DOS to be responsive to their requests, DAG disregarded those blackout periods on multiple occasions and submitted many queries to us during those times, including seventeen additional requests for information, some of which had multiple subparts, all

submitted to us in the spring 2019, despite us having to oversee at least five special elections in addition to the primary election in the month following their requests.

Four of the requests were for information related to ongoing litigation, which also required close consultation with counsel, and at least two requests were for information that DOS explicitly told the DAG it could not provide. One particular data request related to ERIC program data that required DOS to facilitate a separate non-disclosure agreement between DAG and ERIC. In addition, DOS responded to several redundant requests by indicating that the information requested was provided to DAG as part of earlier responses from DOS. Though DOS did not in every case request an extension in writing, DOS staff regularly communicated to DAG staff the status of those requests that required additional review or substantial redaction.

Conclusion Bullets pp. 17-18

- DOS's preliminary data analysis of DAG's data and conclusions causes DOS to conclude that DAG appears to have made significant errors and/or omissions throughout its analysis, which could have been explained to DAG and avoided if they would have shared their data analysis prior to the report draft. More details are enumerated below in Finding 2.

- As described in detail on pp. 1-4 above, as well as in Exhibit A, *Letter from the PA Interagency Election Security and Preparedness Workgroup*, the Commonwealth utilizes leading information technology security practices and controls, using a multi-layer, strategic approach – leveraging people, policies, technologies, best practices and procedures around the safeguarding of data and the protection of the applications, systems and resources.

- DOS shares DAG's concerns about ensuring the most accurate voter records, and the SURE system reaching the end of its useable life. It was for these and other reasons that we had already begun the process of seeking to replace the SURE system and had requested this audit to help gather information to use for the RFP and transition to a new voter registration and election administration system.

- DOS agrees that incorporating additional edit checks and other improvements into the design of the replacement voter registration system will reduce errors and improve accuracy. DOS had previously incorporated these requirements into our RFP for the new system prior to the report draft, as well as other tools that will provide improved checks, balances, and controls.

- We agree that source data or documents should be maintained and accessible for all records and have built these controls into our RFP for our replacement system. Additionally, as noted in our earlier response regarding Scope Limitation B, DOS currently maintains source data for both Motor Voter applications and Online Voter Registration applications.

- DOS is reviewing and working to update current job aids, training, and other guidance to the counties for use of the SURE system and related tasks. Further, these documents are always updated if there are new processes or system functionality changes. DOS also built in requirements regarding job aids and system training into the RFP for the new voter registration and election administration system.

Recommendations

1. As described in detail to DAG throughout the audit, including via hundreds of pages and hours of presentations, affidavits, and materials, including actual redacted weekly and annual independent assessments, testing, and recommendations by DHS and expert third party examiners, the Commonwealth has already and continues to employ these best practices.

2. As stated above on pp. 9-11, we stand firmly behind our decision to maintain the protection of the Commonwealth's critical infrastructure information. Furthermore, our decision is strongly supported by the Commonwealth's security and preparedness experts, concurring with our protection of these documents and determination that we could provide only redacted copies of this information to DAG. As stated in Exhibit A by the Election Security Workgroup, "We believe [DOS's] actions embody and uphold the highest standards of security protocol for the Commonwealth."

3. Please see the response to recommendation 2, noted above. Further, and as referenced in page 14 of DAG's report, access to Protected Critical Infrastructure Information (PCII) was denied because DAG does not perform homeland security duties, nor did it need to know the information to complete the audit. References to the USA Patriot Act and to the Critical Infrastructure Information Act of 2002 (CHA) were provided.

Additionally, it is DOS' position that the Critical Infrastructures Protection Act of 2001, 42 U.S.C. §§ 5195 – 5197h, the related Protected Critical Infrastructure Information (PCII) program, the sensitive nature of PCII information as submitted by DOS for Department of Homeland Security Review, and the Traffic Light Protocol (TLP) information protection protocol and its related "Need to Know" mandate for information considered "For Official Use Only" (FOUO), all provide a mandate to ensure security information is jealously protected. The definition of FOUO contained in Department of Homeland Security Management Directive MD 11042.1 underscores this approach when it provides, in part, that disclosure of such information "could adversely impact . . . programs or operations essential to the national interest." Moreover, the Cybersecurity Information Sharing Act of 2015, 6 U.S.C. §§ 1501-1510, and the Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 671 – 674, both underscore the severe vulnerabilities that exist in critical infrastructure, the need to protect cyber, critical infrastructure and related information, the methods created for such protections, and the duties incumbent upon the holders of such information to limit disclosure solely to those entities having a demonstrated need for the information. Further, Pennsylvania's Right to Know Law, 65 P.S. §§ 67.101 – 67.3104, provides support for the confidential treatment of such agency information, containing numerous exceptions from public disclosure for different categories of records at 65 P.S. §

67.708(b), including homeland security, physical and infrastructure details, threat assessments, public safety matters, computer and related system security, critical systems configurations,

4. As we did throughout this audit engagement, DOS will encourage counties to cooperate in audits and other performance reviews that can benefit them.

5. Please see above pp. 9-11, Exhibit A, and answers to the recommendations above.

6. Results of assessments and recommendations are already shared with those charged with security and governance of the SURE system.

III. **Finding 2** – Data analysis identified tens of thousands of potential duplicate and inaccurate voter records, as well as nearly three thousand potentially deceased voters that had not been removed from the SURE system.

DAG did not provide DOS with the data they identified for us to check until October 9, 2019 and neglected to provide the queries used to complete their analysis for verification even though it had been requested on August 19. Furthermore, the October 9th data received from DAG required extensive cleanup and formatting by DOS before DOS could begin to review their findings. Despite this, they refused to give us a deadline beyond October 28 to respond, notwithstanding DAG's own staff acknowledged that it would take many months to analyze this data and these queries. Remarkably, DAG refused also to extend the deadline beyond Election Day, even with their explicit awareness that the very same DOS and county election staff who are working hard to administer and secure the elections November 5th, are the people needed to respond to DAG's inquiries. DAG apparently decided it was a higher priority to respond to their queries than to administer and secure our elections.

As a result of this unreasonable time period, to date we were only able to assess a small portion of DAG's allegations. Nonetheless, DOS's preliminary data analysis of that small portion of DAG's data and conclusions causes DOS to conclude that DAG appears to have made significant errors and/or omissions throughout its analysis. Consequently, DAG incorrectly flagged thousands of records as potential concerns that through further investigation should not be flagged, including flagrant errors such as identifying individuals who are very much alive as deceased voters.

We will continue to work with the counties to analyze and respond to all DAG's data and queries over the coming weeks and months but have serious concerns about the accuracy and the veracity of the data outlined in this report.

Moreover, regarding the delay in providing electronic files, DAG requested a copy of the voter registration records for SURE; however, within those records is confidential data and information from ERIC. As such, before release of the files and for DOS to not breach its own Non-Disclosure Agreement (NDA) with ERIC, it was necessary for DAG and ERIC to negotiate

an NDA to protect ERIC's confidential data and information from disclosures that would compromise the security of the data and the privacy of individuals whose data resides in ERIC's database. This negotiation occurred over the course of about three months, with DOS diligently facilitating the exchange of information between the parties. The NDA (and not DOS) was the sole reason for the delay in providing the electronic files to DAG.

24,408 cases - the same DL number listed in more than one voter record

Due to the unreasonable time frame provided, data formatting issues with DAG's data production, and the upcoming election requiring our attention, DOS was unable to review this data prior to the deadline for initial response. We intend to review this data analysis in the coming weeks.

13,913 Potential duplicate cases

Due to the unreasonable time frame provided, data formatting issues with DAG's data production, and the election requiring our attention, DOS was unable to complete our review of this data set in the inadequate time frame provided. However, DOS was able to carefully review portions of this data and our initial analysis demonstrates that DAG appears to have made significant errors and/or omissions throughout its analysis, and incorrectly flagged thousands of records as potential concerns that through accurate analysis should not have been flagged. DOS focused its initial review on one of the data sets in DAG's analysis, which is comprised of 1,612 potential duplicate records. A summary of our preliminary results is listed below.

	Matching Elements			
	First Name, Last Name, and DOB	First Name, Last Name, and last 4 SSN	First Name, Last Name, DOB, and Last 4 SSN	Total
Total Potential Matches Analyzed	712	896	4	4
(number of records in potential matches)	(1,426)	(1,795)	(8)	(3,229)
Clear Non-Matches	696	894	0	1,590
Requires further information from the counties	16	2	4	22

During our review, it became abundantly clear that the DAG failed to incorporate all data that was provided to them to validate potential matches. For example, when matching on 3 elements (First Name, Last Name, DOB), DOS could clearly demonstrate potential matches were incorrect when also reviewing the last 4 SSN on the individual's record or DL. DOS was also clearly able

to identify a potential match was incorrect when reviewing an individual's middle name and suffix on a potential match. Despite having this information in their possession, DAG irresponsibly failed to utilize this necessary data to accurately match voter records.

As shown, DOS could clearly demonstrate potential matches were incorrect when matching on SSN in addition to the First Name and Last Name. We were able to do so by using a combination of DL, DOB, or other name elements like middle initial and suffix. Only 2 records in that category require county research.

If a match is underdetermined by DOS, it has been referred to the county for additional research so they can review the documentation available on the voter record.

In summary, when reviewing this group of 1,612 alleged matches by DAG, only 22 were referred to counties for additional information, and based on the results to other data reviews discussed below, we expect most, if not all of these to be cleared by further data. We will complete this review and update this response when we receive responses from county election offices.

6,876 potential DOB inaccuracies – DOBs equate to voters being 100 years or older

Due to the unreasonable time frame provided, data formatting issues with DAG's data production, and the upcoming election requiring our attention, DOS was unable to complete our review of this data set. We intend to review the findings in the coming weeks. However, it is important to note that while there could be DOB inaccuracies related to legacy data, some of the records that were identified as erroneous dates of birth are in fact correct. DOS has a policy for county election officials to comply with Act 188 of 2004, which is otherwise known as the Sexual Violence Victim Address Confidentiality Act. It's an important policy to protect victim information, and it requires county election officials to list a generic date of birth to safeguard their personal information.

2,230 potential DOB and/or registration date inaccuracies

Due to the unreasonable time frame provided, data formatting issues with DAG's data production, and the upcoming election requiring our attention, DOS was unable to review this data prior to the deadline for initial response. We intend to review this data analysis in the coming weeks.

2,991 potentially deceased voter records

Due to the unreasonable time frame provided, data formatting issues with DAG's data production, and the election requiring our attention, DOS was unable to complete our review of this data set within the inadequate time frame given. However, DOS was able to carefully review portions of this data, and in a matter of a few weeks completely disproved multiple

allegations, demonstrating how flawed and unreliable their data analysis was and is. Many of the voter records identified by DAG seemed to confuse voters with same or similar names, which may well have been avoidable with closer analysis of the data DAG had in their possession. Based on our analysis to date, we have every reason to expect that DAG'S allegations will continue to be disproven.

Recommendations

DOS is currently reviewing the data provided by DAG to determine whether any of the DAG's conclusions are accurate when compared to the original voter data provided by DOS. DOS will investigate any apparent DL matches and work directly with counties and PennDOT to verify, as necessary.

1. DOS will continue to leverage its membership in ERIC to identify and review and cancel in-state and cross-state duplicate voter records.

2. As is already current practice, DOS will continue to utilize its membership with ERIC to analyze SURE voter records to identify incorrect, out-of-date or duplicate data in SURE. In addition, DOS will be incorporating additional data cleansing in its implementation of data migration to the new voter database. Further, DOS takes data cleaning and analysis seriously and has hired a data specialist to assist with existing data reviews and migration to the new system.

3. As is already current practice, DOS will continue to employ field-level data validation, as necessary, to give counties the tools they need to identify potential duplicate data, without removing the counties' statutory authority to determine the qualifications of individual applicants.

4. As noted previously, DOS consults with the members of the SURE Advisory Board on an ongoing basis to update the user manuals, job aids and directives that counties rely on to guide them through all aspects of maintaining accurate voter records SURE.

5. Pursuant to DOS's existing agreement with ERIC, DOS will continue to send data to ERIC for the purpose of identifying potential in-state and cross-state duplicate voter records. DOS will also direct counties to use the duplicate voter record notices developed for the ERIC program to conduct regular list maintenance in compliance with federal and state law. Also, as mentioned above, DOS will leverage the new data specialist position to assist with periodic system data analysis.

6. As is the typical procedure of DOS, work with counties to conduct data cleanup will continue, as necessary, to identify and correct data entry errors and bad data migrated from legacy voter registration systems.

7. DOS requirements for the new voter registration system, which were developed in consultation with county voter registration and election personnel, require data validation measures to reduce the likelihood of data entry errors. DOS will also continue to development its online voter tools, like Online Voter Registration and Online Absentee Ballot Request, which provide upfront verification for many voters and eliminate manual data entry.

8. Though it appears from our early analysis that the number of potentially deceased voters is vastly overstated due to a flawed data analysis, DOS will continue to work with counties to research the data provided by DAG to identify and remove any apparent deceased voters.

9. In keeping with current protocols, DOS will continue its collaborative work with the Department of Health and ERIC to identify deceased voter records and transmit to counties the information they need to remove them.

10. DOS will continue to collaborate with DOH to identify process improvements and data enhancements to ensure that counties have timely and correct information about potentially deceased voters.

IV. **Finding 3**- The Department of State must implement leading information technology security practices and information technology general controls to protect the SURE system and ensure the reliability of voter registration records.

As described in detail on pp. 1-4 above, as well as in Exhibit A, *Letter from the PA Interagency Election Security and Preparedness Workgroup*, the Commonwealth utilizes leading information technology security practices and controls, using a multi-layer, strategic approach – leveraging people, policies, technologies, best practices and procedures around the safeguarding of data and the protection of the applications, systems and resources.

As noted on page 33 of the DAG report, Governor Wolf signed Executive Order 2016-06, which effectively consolidated and centralized management and operation of IT services for all executive agencies. This model over time has led to improvements in overall IT governance and the implementation of additional internal and external controls. DOS, like any other executive agency, conforms to the IT Policy Governance structures set forth in IT Policy BUS000 (ITP-BUS000), which can be found online here:
https://www.oa.pa.gov/Policies/Documents/itp_bus000.pdf

Consistent with its charge under ITP-BUS000, the CIO for the Employment, Banking and Revenue Delivery Center, of which DOS is a part, holds regular steering committee meetings with DOS, Delivery Center IT staff, and DOS IT support staff to ensure alignment between the Commonwealth's IT policies and DOS's strategic and operational planning.

Vendor oversight practices

Per ITP-SEC009, all employees, including contractors, providing IT services must complete a criminal background check. Those background checks are completed by the Pennsylvania State Police (PSP). Further, all employees or contractors must comply with the Department's TLP Policy related to critical infrastructure information. Additionally, SOC reports are currently reviewed by personnel within the EBR Delivery Center and Office of Administration. Further, DAG requested SOC reports from vendors that were a non-party to our Interagency Agreement, and therefore, was not in scope.

DOS management's county-level SURE Equipment Use Policy fails to provide clear guidance to counties.

DOS's SURE Equipment Use Policy contains instructions for county election and county IT officials regarding proper connectivity and proper use of SURE equipment, as well as guidance regarding the use of county-owned equipment. As noted in the DAG report on page 35, DOS's policy includes certain prohibitions that have been put in place to protect SURE equipment and the SURE network. In addition, the policy states on page 7 that county staff are required to notify DOS of any changes that may impact the SURE system in any way at least one week prior to implementation of those changes. Please refer to the relevant excerpt from the policy below:

Very Important: County staff are required to provide DOS with at least one-week notice of any planned changes that may impact the SURE system in any way (e.g. planned power outage, relocation of equipment, etc.). County IT staff are also required to notify DOS of any emergency changes that impact the SURE system in any way. Notification of changes may be made via the SURE Help Desk. Failure to notify DOS of changes will result in the county bearing any costs incurred to identify and resolve any problems that occur.

Currently, the policy directs counties to contact the SURE Help Desk to provide notification of planned changes. The moment that a county contacts the SURE Help Desk, the Help Desk technician creates a "service ticket" in DOS's ticketing system. The Help Desk technician also records the details provided by the county, and either resolves the issue or escalates the ticket to Tier 2 Support staff. The ticketing system is the logging and monitoring tool that agency users and support staff MUST use to log, update, and track SURE-related. This single logging and tracking system is in place to promote accountability and to ensure continuity throughout the routing of the ticket. It also serves as a knowledge base that enables DOS staff to reconstruct the actions taken from the moment a ticket is opened until the ticket is resolved.

We agree that it is necessary to regularly review and update the Equipment Use Policy, which is already in progress. We also agree that providing a form to formalize county configuration requests could augment the current system by serving as the original artifact of a county's request. As a result, we will distribute a link to the policy in the body of every SURE maintenance memo.

Though the DAG's report provides no specific recommendations for updates to the policy, DOS will nonetheless review the current version of the policy to determine what additions or clarifications may be necessary to make clear the risks of not following the policy.

Recommendations

1. As noted in our responses to requests for information 13 and 14, section 1302-C, 25 P.S. §3150.2, provides for a SURE Advisory Board to advise DOS on matters related to the SURE system and voter registration. The six members of the Advisory Board are selected by the Secretary of the Commonwealth and the majority and minority leaders in the two houses of the General Assembly. As articulated in the Board's charter, the Advisory Board and DOS conduct monthly teleconferences to:

- advise DOS so that it can provide the most effective and efficient statewide voter registration system for the Commonwealth of Pennsylvania.
- provide recommendations regarding issues and procedures related to SURE system maintenance and future enhancements.
- provide feedback during the development of new SURE processes to improve the performance of the SURE database, to comply with statutory changes, and to anticipate the future needs of users and stakeholders.
- document and improve existing business processes to make the best use of SURE system technology.
- assist in prioritizing requests for SURE system improvements and changes.
- oversee and direct, as necessary, both government and public SURE user groups.
- work with county election officials, in addition to those on the Advisory Board, to gain consensus on issues affecting SURE.
- assist DOS in designing a communications strategy to effectively reach county election officials, other SURE users, and the public at large.

The monthly teleconferences, except when a month falls during a statewide election, include members of DOS staff, as well as the Department's Project Management Office's Portfolio Manager who serves as the primary liaison between DOS staff, Help Desk support and OIT.

2. When the Department of State was incorporated into the Employment, Banking and Revenue (EBR) Delivery Center, it allowed OA/OIT resources across multiple EBR agencies to start supporting DOS IT activities, including SURE system maintenance. One of the first changes implemented was the removal of Production system access from the primary vendor supporting SURE. Other contracted resources from different vendors (under the management of Commonwealth IT staff) still had access, but required explicit, written approval from DOS and IT Management staff prior to making any changes.

As part of an effort to modify how IT support and maintenance services were provided to DOS, a Request for Proposal (RFP) was issued, including significant changes to how services are being delivered to DOS. This will include (but not be limited to) new documentation requirements, new processes and policies, and an increased ability to monitor and oversee vendor staff working on the systems. Several of the more significant changes include; moving vendor staff into Commonwealth facilities where there will be in-person supervision from IT management staff; utilizing equipment issued, maintained and monitored by Commonwealth IT resources from OA

and the Delivery Center; and the addition of Service Level Agreements (SLAs) requiring greater accountability regarding testing and oversight of system changes.

Another aspect of adding DOS to the EBR Delivery Center is that DOS can incorporate the IT best practices developed over time by the larger EBR DC agencies. This enables DOS-specific IT support practices to mature much more quickly than they could as a stand-alone agency. The new maintenance contract will give DOS greater ability force the vendor to adopt these policies and practices moving forward.

As noted in our response to the DAG's discussion of the governance structure of SURE on pages 32 through 34 of its report, DOS and the CIO for the Employment, Banking and Revenue Delivery Center, of which DOS is a part, conforms to the governance structure established by ITP-BUS000. We appreciate the perspective of DAG regarding employee awareness of the governance structure and how effectively team members are working within that structure. DOS will continue to work with OIT to ensure that all staff working in and supporting SURE are fully aware of the governance structure, understand its lines of authority and communication, and understand expectations regarding how they are to operate within the governance structure.

3. We are in the RFP process for replacement of the SURE system. Please refer to our response on page 8, which outlines the general timeline for the RFP.

4. Many of the security guidelines issued by DHS-CISA in May 2019, *Best Practices for Security Election Systems*, are already part of the library of election security practices and protocols that we already use, and the agency and the Commonwealth are always evaluating opportunities to implement additional controls that improve the security posture of the environment. As described in detail on pp. 1-3 above, as well as in Exhibit A, Letter from the PA Interagency Election Security and Preparedness Workgroup, the Commonwealth utilizes leading information technology security practices and controls, using a multi-layer, strategic approach – leveraging people, policies, technologies, best practices and procedures around the safeguarding of data and the protection of the applications, systems and resources.

5. Vendors are already required to comply with Commonwealth security policies. External suppliers must agree to, and comply with, the Commonwealth IT contracts terms and conditions which requires compliance with Commonwealth information technology policies (ITPs), non-disclosure agreements (NDAs), IT Acceptable Use agreements and audit requirements. Additionally, DOS has agreements in place with agencies and external partners that govern the security, confidentiality and audit provisions as applicable. Further, all vendors who provide IT services must comply with background checks. Additionally, all vendors and Commonwealth employees comply with annual security training requirements.

6. Vendors already are monitored in compliance with management directive 325.13. DOS and the Commonwealth monitor external supplier controls by requiring the delivery of Service Organization Controls (SOC) reports as part of the contract with the data center service provider.

7. As noted in our prior responses, DOS maintains agreements with agencies and external partners that govern acceptable use, security, confidentiality and auditability. The Commonwealth also requires delivery of SOC reports by suppliers be reviewed timely and collaboratively by DOS and OIT to ensure full accountability from internal and external partners.

8. Please see prior section pp. 20-21. DOS agrees that requiring counties to formally acknowledge the policy periodically will ensure awareness and accountability. It is important to keep in mind that the network through which counties connect to SURE is maintained entirely by the Commonwealth and remains segregated from county and other networks. Should a county attempt to reconfigure its connection to the SURE network, DOS is alerted via network monitoring. See below for more details.

9. Whenever a county requires equipment, the county submits a request form to the SURE office. If the request is approved, a ticket is entered in ServiceNow and assigned to the SURE Tier 1 help desk. The requested equipment is provided by the Commonwealth and sent to the requesting county. A few of the counties procure their own high-volume printers. Request for approval to use any county-owned equipment follows the same process as requesting Commonwealth equipment.

The county networks connect to the County Connect Network via a hub (owned by the County or the Commonwealth) connected to a Verizon router under Commonwealth control. It is the single point of connection between the Commonwealth network and the county network. There are no permitted deviations from this architecture model.

Some of the counties use Commonwealth-provided KVM switch to attach mice and keyboards to the Commonwealth WinTerms, others connect county-owned peripherals directly to the WinTerm.

10. DOS SURE staff and the Bureau of Management Information Systems (BMIS) are working together to review and update the SURE Equipment Use Policy and associated procedures. This project is anticipated to be completed by the end of the year. Part of the policy changes will include having all appropriate SURE users sign the policy.

11. Part of the initiative to update this policy as described above includes the review and revision of the *SURE User ID Request Form*.

12. DOS provides SURE system policies to counties via the SURE Extranet, but we will better organize them and will also leverage the CCAP Election Security Workgroup to ensure awareness and understanding of the policies among all relevant county personnel.

V. **Finding 4** - Voter record information is inaccurate due to weaknesses in the voter registration application process and the maintenance of voter records in the SURE system.

Weaknesses within application process

We strongly disagree that there are significant weaknesses in the voter registration process. In fact, DOS has made and continues to make improvements to the application process and county processing efforts.

We agree that additional edit checks are warranted, and we had already incorporated these and other protections into the RFP for the new voter registration and election administration system that will replace the SURE system. DOS shares the Auditor General's concerns about accuracy and is taking steps to make sure that the new system with provide more robust checks and balances.

DOS had also already integrated automated processes, such as checking for duplicates and running reports, into the RFP for the system that will replace SURE. We intend to move to a system that will provide readily configurable hard stops that will not allow the user to proceed to the next step in the process without completing certain items, like pending applications or upload of source documents. We also intend to do a thorough data analysis prior to moving to a new system so that we are starting with the most accurate data possible in the new election administration system.

Weaknesses regarding maintenance of voter registration records with SURE system

List maintenance was an area DOS focused on heavily in requirements development for the new system. Additionally, DOS is seeking a system that allows for better oversight by DOS and county election officials, including pulling status reports and receiving automated notifications when a process is completed or when a deadline is approaching, and a process remains incomplete by a county.

DOS is seeking a system that allows better visualization of the data for internal and external users. Additionally, DOS hired a data specialist who will assist with analyzing data within the system to identify areas for improvement as well as trends that may enable to DOS to identify efficiencies or areas where additional training is needed by county users. The data specialist will also assist the new "SURE" team in monitoring user activity and flagging incomplete processes, incorrect actions and overdue tasks.

We appreciate the Auditor General's recommendation, but also note that our use of data is impeded by the current language in the Act 2002-3, the voter registration law. DOS continues to work to find ways to use as much of the data we receive from ERIC as possible, while we engage with the Legislature to get the necessary changes to the law.

Applications remain in pending status

DOS has worked proactively to address the issue of applications that remain in pending status. As noted on page 42 of the DAG report, DOS works with counties to "clear" pending applications before closing registration prior to a primary or general election. It is not uncommon for there to be thousands of applications that are still in New or Pending at and immediately after

the voter deadline. Between October 9, 2018 and November 5, 2018, the counties processed 13,130 pending applications.

To reaffirm that counties may not leave voter applications in pending status for long periods of time, DOS issued a directive on July 10, 2018, directing counties to make sure that all New and Pending applications are resolved prior to closing registration. DOS also sent a subsequent memorandum and copy of the directive on October 16, 2018 to remind counties of their statutory obligation to process all pending applications. In addition, the Division of SURE also includes a section in its SURE-related preparations memorandums distributed prior to each primary and election reminding counties to process all new and pending applications before closing out registration. In 2019, these memorandums were distributed to counties on April 24 and October 7. The Department also directly calls each county with pending applications to ensure they are processed prior to printing supplemental poll books so all eligible voters are listed in the poll book.

In the event that any counties have not resolved all of their New and Pending applications by the Monday prior to the election, DOS distributes through SURE a list of all applications in these two statuses, with an additional reminder to resolve those applications and a reminder to rely on those lists as a resource when they are adjudicating provisional ballots.

Recommendations

1. We will take this recommendation under advisement and discuss this with the SURE Advisory Committee.

2. We will take this recommendation under advisement and discuss this with the SURE Advisory Committee.

3. DOS disagrees with DAG's recommendation to the extent it relates to rejecting voter registration applications in a pending status for non-match of numbers. To reject such applications would be contrary to DOS's directive to the counties that there is no legal basis under federal or Pennsylvania law to reject or delay processing a voter registration application solely based on a non-match between a registrant's identifying numbers on the application and the comparison database. As it relates to other pending applications, DOS will review DAG's recommendation in consultation with legal counsel as we implement the new election administration system.

4. We will take this recommendation under advisement and discuss this with the SURE Advisory Committee.

5. We have existing procedures in place but will take this recommendation under advisement and discuss this with the SURE Advisory Committee.

6. DOS provides to counties annually the data and guidance necessary to complete their statutorily-mandated list maintenance duties, which require counties to send NVRA-compliant notices to voters who appear to have moved or who have not voted or otherwise updated their voter record in the five years preceding the date of the notice. The deadlines to complete these list maintenance activities are defined by statute. Both federal and state law establish "quiet periods" within 90 days of an election, before which counties need to complete their annual statutory voter removal programs, otherwise known as list maintenance. So, it's important to note while the DAG alleges records may not have been inactivate or removed, a majority of county offices may not have completed their list maintenance activities until after the 2018 General Election, which fell after they received the datasets from DOS. This is all to say that additional records may have been inactivated or removed for lack of activity after the General Election, but the datasets didn't capture that data as they were current as of October 9, 2018.

As demonstrated in our response to RFI #10, the counties' list maintenance activities are monitored daily via an automated job that summarizes each county's list maintenance activities. These list maintenance activities, with counts of inactivated and cancelled records, are summarized in the DOS's annual report to the General Assembly on voter registration.

DOS will continue to work with SURE Support staff to further develop these automated monitoring notifications, and we will work with the SURE Advisory Board to augment our guidance, as necessary.

7. Please refer to the automated monitoring description provided in our prior response.

8. We have been working towards this goal, and in fact, were already planning to implement extended ERIC functionality in December 2019, having now acquired all the necessary prerequisites for full functionality to take effect.

VI. Finding 5 - Incorporating edit checks and other improvements into the design of the replacement system for SURE will reduce data errors and improve accuracy

Features that were missing or inadequate within the SURE system which could reduce or prevent errors

DOS already included requirements in the RFP prior to this report for the new system to address and prevent errors, including residential address checks. Until the new system is implemented, DOS will work on implementing a feature in the SURE system that does not allow for a residence outside of the PA.

Like most state election offices nationwide, DOS is in the process of incorporating GIS into all processes where applicable. GIS will be a feature of our new election administration system but was not widely used when the SURE system was built. We agree that it is useful and necessary, in fact, it is so important to DOS that we recently hired a Data Specialist with GIS expertise to our elections team, to help with data analysis, data visualization and GIS implementation.

We are also working with counties on a GIS pilot to develop procedures related to redistricting and use of GIS in elections for residential address verification and other means. The pilot is organized with both state and county representatives with both elections and GIS experience. We anticipate the first GIS procedures will be available in 1st quarter 2020. The pilot also builds off national expertise where Pennsylvania Department of State was recently selected as one of five states to further geo-enabled elections with the National States Geographic Information Council (NSGIC).

https://elections.nsgic.org/five-statewide-pilot-studies-launched-to-further-geo-enabled-elections/

DOS is aware of the lack of "read only" features and spent considerable time during requirements development for the RFP drafting user roles and functions tied to those roles, including read only access. These user roles would allow for better definitions of access for each user as well as allowing better tracking and auditing of the actions each user takes in the system.

Finally, like several other areas already discussed, DOS considered and is requiring several edit checks and hard stops for the new election administration system. In addition to not being able to move forward in certain processes until all information is complete, DOS will "lock" certain areas or functions of the system during certain periods. This will make it impossible for counties to revise or cancel records during certain periods.

Two areas of improvement related to PennDOT Motor Voter process and reporting capabilities within SURE system

DOS has a strong working relationship with PennDOT and has spent considerable time in the last several years improving the Motor Voter process, including changes to the order of the screens and simplification of language used in the Motor Voter system. DOS is currently working with PennDOT on the next round of improvements to the process, which already include potential updates to the change of address matter as identified in the audit report. Additionally, the Department wishes to further simplify the voter registration process at PennDOT and streamline the experience for individual's registering to vote or updating their existing registration.

DOS is very aware of the limitation regarding creation of reports in the SURE system. We are working with developers to write scripts for the most common reports needed from the current system, but also included requirements regarding report generation in the RFP for the new system. We agree that all users need to be able to run customized reports and have prioritized that need for the new system.

Recommendations

1. We acknowledge the recommendations made here and are happy to report that all the following items are already requirements for the new election administration system:

- GIS feature for checking voter addresses, assigning polling places to voters, locating polling places, etc.;
- Edit checks and system stops to alert users of out of state addresses, incomplete information, missing information, the need to upload supporting documents, etc.;
- User roles that allow DOS to create different levels and types of access, including read only access, for system users;
- Hard stops that prohibit users from moving to the next process before completing the current one and that do not allow users to take actions outside of allowed timeframes;
- The ability to generate notifications (emails and letters) automatically and in batches from the system, including notices to those who submit a change of address, but are not currently registered;
- And giving each user the ability to generate reports that contain information that they need rather than requesting report generation through a ticket process to the Help Desk.

2. Due to the unreasonable time frame provided, data formatting issues with DAG's data production, and the upcoming election requiring our attention, DOS was unable to review this data prior to the deadline for initial response. We intend to review this data analysis in the coming weeks and will follow up with the county, as necessary.

3. Due to the unreasonable time frame provided, data formatting issues with DAG's data production, and the upcoming election requiring our attention, DOS was unable to review this data prior to the deadline for initial response. We intend to review this data analysis in the coming weeks and will follow up with the county, as necessary.

   The SURE system is designed to automatically associate the proper cancellation reason with the source of the cancellation transaction. For example, voter records that are being cancelled as a result of statutory list maintenance activities are automatically coded with the cancellation reason CANCEL-INACTIVE STATUS FOR TWO FED GEN ELECTION CYCLES and voter records that are cancelled due to a Department of Health death notification are automatically coded with the cancellation reason CANCEL – DOH DEATH NOTIFICATION. DOS will continue to work with the SURE Advisory Board to build in data field validations as necessary, and we will continue to provide step-by-step training and written instructions for county SURE users.

4. Please see our response on page 28. We are currently working with PennDOT to streamline and further enhance the existing registration process, which contemplates updates to the change of address process to capture additional registration information so the county may process a new registration if the applicant thought they already had an existing registration.

VII. Finding 6 - A combination of a lack of cooperation by certain county election offices and PennDOT, as well as source documents not being available for seventy percent of our test sample, resulted in our inability to form any conclusions as to the accuracy of the entire population of voter records maintained in the SURE system.

As noted in our response to Scope Limitation B on pages 11 and 12, it is not accurate to state that there is not source documentation available for Motor Voter and Online Voter Registration applications and the source data necessary to test the accuracy of 93 Motor Voter records and 19 Online Voter Registration records was available to the DAG. See above pp. 11-13. We offered copies of the source data available in SURE for Motor Voter applications, but the DAG declined.

While DOS has provided retention guidance previously, we do believe we could expand that guidance. The County Records Manual is the primary resource of guidance on the retention and disposition of county records. This manual is posted on the Bureau of State Archives on its website here: https://www.phmc.pa.gov/Archives/Records-Management/Documents/RM-2002-County-Records-Manual-2017-Update.pdf. This manual serves as the comprehensive guide to county records retention requirements, including those requirements for elections and voter registration records. The manual makes clear that applications must be retained for 22 months in accordance with federal and state law. When necessary, DOS collaborates with the Pennsylvania Historical and Museum Commission (PHMC) to update our portions of the guide.

As noted in our response to RFI #15, we distribute the PHMC documents as the authoritative tools for both election and voter registration records retention requirements because they are legally accurate, compiled in subject-specific documents, and they were last updated in consultation with DOS. Though DOS cannot speak to the PHMC's methods or frequency of distribution of the guide, we acknowledge that infrequent distribution of the relevant portions of the guide could contribute to a lack of awareness on the part of county election officials. DOS plans to reissue retention guidelines prior to the end of 2019 as well as post to the County Extranet.

PennDOT refused to provide access to Motor Voter source documents

Please refer to our response to Scope Limitation B on pp 11 - 12.

DOS does maintain online application source documents

As noted in our response to Scope Limitation B on pp 11- 12, DOS maintains source data for both Motor Voter applications and Online Voter Registration applications.

Recommendations

1. DOS does maintain source data for Online Voter Registration applications, and there is an auditable trail of data housed in multiple locations within the SURE architecture.

2. This is not a necessary option because DOS maintains an electronic audit trail as described in the preceding paragraph.

3. We will take this recommendation under advisement and discuss this with the SURE Advisory Committee.

4. DOS will expand our communications to counties on the retention policies mandated by the NVRA and state law, as referenced in the County Records Manual. DOS will post a link to the County Records Manual on our website and the County Extranet, and we will include references to the manual in our training materials.

5. DOS will conduct a review of the SURE regulations, and consider amendments if necessary, to ensure the regulations are consistent with federal and state retention requirements.

VIII. Finding 7 - The Department of State should update current job aids and develop additional job aids and guidance to address issues such as duplicate voter records, deceased voters on the voter rolls, pending applications, and records retention.

Job aids need to be updated to reflect improvements recommended for the SURE system regarding review for duplicate voter records and deceased voters of the voter rolls

As noted in our response to RFI #25, DOS updates job aids at the time functionality is added or changed. These updated job aids are distributed to all county election and voter registration contacts a few days before the added or changed functionality is deployed to SURE, including the Duplicate Voter Notice and Deceased Voter job aids that were updated in August 2017 and July 2019, respectively. Counties are also provided an opportunity to review the new functionality prior to deployment during county user review sessions.

We agree with the DAG that job aids should be dated consistently, with the month, day and year. To ensure that there is no possible confusion, we will also add a version history log to each job aid to clarify changes or modifications. Further, DOS will engage in a review of all job aids and guidance promptly and update accordingly, as needed.

Please refer to our response on page 26 regarding the July 10, 2018 directive issued by DOS related to pending applications.

Recommendations

1. We will continue to offer hands on training at no cost to the counties. Currently, the Department provides on-site training at the county or on-site training in Harrisburg at their request.

2. We agree with the DAG that job aids should be dated consistently, with the month, day and year. To ensure that there is no possible confusion, we will also add a version history log to each job aid to clarify changes or modifications. Further, DOS will engage in a review of all job aids and guidance promptly and update accordingly, as needed.

3. We will take this recommendation under advisement and discuss this with the SURE Advisory Committee.

4. DOS will review this recommendation with legal counsel and determine what guidance DOS can provide as we implement the new voter registration and election administration system.

EXHIBIT A

COMMONWEALTH OF PENNSYLVANIA
INTERAGENCY ELECTION SECURITY & PREPAREDNESS WORKGROUP

October 28, 2019

Auditor General Eugene DePasquale
613 North Street, Room 229
Finance Building
Harrisburg, PA 17120-0018

Dear Auditor General DePasquale:

As the members of the Pennsylvania Inter-Agency Election Security and Preparedness Workgroup, we strongly disagree with many of the findings of your Draft Performance Audit report relating to the Department of State's SURE system.

The Commonwealth takes its responsibility to protect the vote very seriously. Pennsylvania is proud to lead the country in using strategic partnerships with federal, state, and county officials, along with partners in the private sector, to deploy election security best practices and innovative responses to the ever-changing world of cyber security threats. Based on our extensive security and preparedness experience, we find many of your audit findings to be flawed and misleading, failing not only to accurately reflect the strength of our security protocols, but also the vital importance of protecting our nation's critical infrastructure information as crucial to defending our nation's security.

As evidenced in hundreds of pages and hours of presentations, affidavits, and materials shown to your office, the Department of State (DOS) and the Office of Information Technology (OIT), in partnership with all other members of the Inter-Agency Election Security and Preparedness Workgroup, employ leading information technology and other security practices and controls to protect the Commonwealth's elections. The Commonwealth's strong security protocols include but are not limited to the following:

- We engage in 24/7 continuous network monitoring, constant contact with the Center for Internet Security's Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), inventory identification, intrusion detection sensors, infrastructure/network diagrams, regular third-party vulnerability and cyber assessments, firewalls, encryption, password protection and multi-factor authentication in access to email, file storage, systems, and other resources.

Office of the Secretary of State
Room 302 North Office Building | 401 North Street | Harrisburg, PA 17120-0500 | 717.787.6458 | F 717.787.1734 www.dos.pa.gov

- The Commonwealth utilizes multiple layers of protection, controls, and end-user security awareness training, risk management, policy compliance assessments, continuity of operations (COOP) planning, disaster recovery, and code reviews and scans as part of a comprehensive cybersecurity program.

- Pennsylvania continues to be a nationally recognized and award-winning leader among states in cybersecurity. Our extensive collaboration, including the formation of this workgroup in 2018, is considered a notable model that many other states are interested in replicating. In addition to DOS, OIT, and the Governor's office, our multi-layered and cross-sector partners include the U.S. and PA Department of Homeland Security, Pennsylvania Emergency Management Agency (PEMA), Pennsylvania State Police, Pennsylvania Department of Military and Veterans Affairs, Pennsylvania Inspector General, County Commissioners Association of Pennsylvania (CCAP), and Center for Internet Security (CIS), among others.

- Beginning in the 2019 primary, our teams moved our election-day operations to PEMA headquarters. To strengthen our security and responsiveness and enhance our collaboration and coordination, the Commonwealth's election experts, security teams, call center, cybersecurity experts, law enforcement, and state emergency personnel are now able to closely monitor developments throughout the day from one location with all of PEMA's resources close at hand. Our election, security, and preparedness professionals also participate across the state and across the country in real-time information-sharing on cyber issues, as well as on-the-ground and weather-related situations that could impact voting.

- The Commonwealth also provides anti-phishing and security training and tools to all 67 counties at no cost to them, and our state and federal partners such as the U.S. Department of Homeland Security and the Pennsylvania National Guard additionally offer vulnerability and cyber assessments to them at no cost. Furthermore, we have collaborated with all these partners on multiple tabletop exercises for counties and partners modeled after law enforcement and emergency response techniques, to train election, IT, and security personnel in incident response and preparation, simulating scenarios that could impact all aspects of voting operations. Pennsylvania stands out as a leader nationwide in the extensiveness of our cross-sector training, coordination, and collaboration.

- Last spring, DOS directed the counties to select new voting systems meeting current security and accessibility standards with voter-verifiable paper trails by December 31, 2019 and implement them by the 2020 primary. All these new systems were subject to penetration testing, access control testing to confirm detection and prevention of unauthorized access, and evaluation that every physical access point is well-secured and system software and firmware is protected from tampering.

- To date, 79 percent of Pennsylvania's counties have voted to select their new systems. One year ago, 50 out of 67 counties used paperless DRE voting machines. Remarkably, this November, 52 out of 67 counties will be voting on systems with auditable paper records.

- Additionally, In January 2019, DOS formed a post-election audit workgroup, to study models of post-election audits. These audits, such as risk-limiting audits, are scientifically designed and utilize highly effective procedures conducted after an election to strengthen election security and integrity, confirm the accuracy of election outcomes, and provide confidence to voters that their votes are being counted accurately. PA's first pilot RLA audits will be conducted in November 2019 in Mercer and Philadelphia counties. Recently, the Washington Post, in addition to many experts, lauded this post-election audit approach a best practice that all counties across the country should follow.

The Commonwealth has for many years protected documents and other information related to sensitive security efforts and procedures. Developing emphasis at both the federal and state levels in protecting critical infrastructure information has appropriately generated even stronger protocols at all levels, in order to further strengthen our nation's security.

In January 2017, pursuant to the USA Patriot Act, the federal government designated election infrastructure as part of the nation's critical infrastructure. Since that time, federal, state, and local governments have been working to advance policies and procedures as quickly as possible to provide the greatest protection to our elections. Because this designation is so new, these policies and procedures are under constant review and development to be responsive to changing needs and threats.

Late in 2017, the federal government created the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC), a first of its kind collaboration among federal, state, and local officials to secure elections, to formalize and improve information-sharing and communication protocols to ensure that timely threat information, support, and resources reach all election officials so they can respond to threats as they emerge.

When the audit began in 2018, the EIS-GCC was very new, and the development of national and state procedures has grown steadily over the last year. Pennsylvania has worked closely with the federal government and other states to advance these policies, and in August 2019, Acting Secretary Boockvar was named as a representative to the EIS-GCC, on behalf of the National Association of Secretaries of State (NASS).

Protection of critical infrastructure information is and has been one of the essential security protocols recommended by security experts at every level. These significant protections were discussed with your office from the very early communications before the audit even began and continued throughout the audit. As security and preparedness professionals, we cannot emphasize enough how important this protection is in order to carry

out our duty and responsibility to the citizens of our Commonwealth. This means that information such as vulnerability and cyber assessments, system configuration and architecture, disaster recovery plans, and other types of information that relate to our critical infrastructure should under no circumstances be shared with anyone other than those with an absolute need to know in order to perform homeland security duties.

This protection is supported by exceptions in the Pennsylvania Right to Know Law and the federal Freedom of Information Act, as well as protection under the Commonwealth Information Technology Policy ITP-SEC019, the Cybersecurity Information Sharing Act of 2015, the Protected Critical Infrastructure Information (PCII) program, and the federal and Department of State's (DOS) Traffic Light Protocol (TLP) policy.

In fact, the U.S. Department of Homeland Security (DHS) and Pennsylvania have specifically identified for PCII protection and TLP Red designation critical infrastructure documents including, but not limited to, system assessments, phishing campaigns, risk and vulnerability assessments, vulnerability scanning (cyber hygiene), architecture review, and cybersecurity evaluation tools, and DHS has confirmed this protection covers all this information as recently as a few weeks ago.

As security and preparedness experts, we fully concur with the Department of State's and Office of Information Technology's protection of these documents and determination that they could provide only redacted copies of this information to you. We believe their actions embody and uphold the highest standards of security protocol for the Commonwealth.

In closing, based on our extensive experience with election security, we find many of your audit findings to be flawed and misleading, failing to accurately reflect the strength of our security protocols and the vital importance of protecting our nation's critical infrastructure information as crucial to defending our nation's security.

We are very proud to work in partnership with all our member agencies, to leverage our collective expertise in elections, homeland security, cybersecurity, law enforcement, and emergency preparedness, and provide a national model for security protocols and protecting and defending our elections in the Commonwealth. We welcome you and any others willing to join in productive conversations to further our critical collective efforts.

Sincerely,

Major General Anthony J. Carrelli
Adjutant General of Pennsylvania
Department of Military and Veterans Affairs

Colonel Robert Evanchick
Pennsylvania State Police Commissioner
Pennsylvania State Police

Marcus Brown
Director of the Office of Homeland Security
Pennsylvania Office of Homeland Security

Kathy Boockvar
Acting Secretary of the Commonwealth
Pennsylvania Department of State

John MacMillan
Chief Information Officer and
Deputy Secretary for Information Technology
Pennsylvania Office of Administration

Randy Padfield
PEMA Director
Pennsylvania Emergency Management Agency

Bruce Beemer
Pennsylvania Inspector General
Office of the Inspector General

Page 5 of 5

EXHIBIT B

COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF STATE

Testimony of Kathy Boockvar
Acting Secretary of the Commonwealth
Commonwealth of Pennsylvania
Hearing on *Securing America's Elections*
U.S. House of Representatives, Committee on the Judiciary
September 27, 2019

Chairman Nadler, Ranking Member Collins, and distinguished members of the House Judiciary Committee, my name is Kathy Boockvar, and I am the acting Secretary of State (or Secretary of the Commonwealth) of Pennsylvania. As Secretary, I lead the Pennsylvania Department of State (DOS) to promote the integrity and security of the electoral process, protect public health and safety by licensing professionals, support economic and nonprofit development through corporate and charitable registrations, and sanction professional boxing, kick-boxing, wrestling and mixed martial arts. Prior to being appointed as Secretary, I served as Senior Advisor to Governor Wolf on Election Modernization, leading and managing initiatives to improve security and technology in Pennsylvania's elections, in collaboration with federal, state, and county officials.

Thank you for inviting me to testify at your *Securing America's Elections* hearing. As the Chief Election Official of Pennsylvania I have the immense privilege of working with extraordinarily dedicated election directors and personnel in all 67 counties across the Commonwealth, as well as committed Secretaries of State across our great nation, to ensure that our elections - elections that allow candidates running for every local, state, and federal office to serve – are free, fair, secure, and accessible to all eligible voters. In August 2019, I was also honored to be asked to serve as the Elections Committee Co-Chair for the National Association of Secretaries of State (NASS).

The issues surrounding security have made election administration more challenging and complex than ever. As we have learned over the last several years, foreign adversaries and other cyber actors have attempted and continue to attempt to influence elections in the United States. The key to thwarting this effort is that we must continue to build and strengthen our walls faster than those that are trying to tear them down. Election security is a race without a finish line, and our adversaries are continuously advancing their technologies. We must do the same and more; our success is dependent on substantial and sustained dedication of resources.

Alongside the great majority of states across the nation, we urge the federal government to provide additional election security funding and support to counties and states and reinforce our collective infrastructure. All of us at the federal, state, and local levels benefit from the security of our elections, so funding these critical operations must be a cost-share by the federal, state, and local levels. Because the technologies and attempted attacks are becoming more

SECRETARY OF THE COMMONWEALTH
302 North Office Building | 401 North Street | Harrisburg, PA 17120-0500 | 717.787.6458 | Fax 717.787.1734 | dos.pa.gov

sophisticated all the time, we need to plan for and invest in election security like we invest in other ongoing initiatives and challenges. Like other types of security, like STEM fields, like education of our children – investment cannot be once and done, and it should never be dependent on political winds. There is nothing partisan about ensuring that our elections are secure and accessible to all eligible voters. We must have a continuous investment in election security at all levels, both in funding and in strengthening our infrastructure, communications, and responsiveness, so that we may advance and adapt to change as new information is gained and new technologies advanced.

NATIONAL LANDSCAPE

There have been some great advances in election security over the last several years at all levels, while challenges continue to emerge as well. All these – continuing to strengthen advances and pursuing additional goals forward - require significant funding, proactive bi-partisan leadership, quick response time, multi-agency collaboration, and other support.

The National Association of Secretaries of State (NASS), National Association of State Election Directors (NASED) and Secretaries and election officials across the country have been resolute in our commitment to bolstering security in elections, and collaboration at all levels. As NASS Elections Committee Co-Chair, I look forward to working with my fellow Co-Chair Secretary Mac Warner (W.Va.) and with colleagues across the country, to share best practices and provide the most secure and accessible elections to eligible voters in Pennsylvania and nationwide. One of my responsibilities as Co-Chair is to serve as a NASS representative on the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC).

In January 2017, when the federal government designated election infrastructure as part of the nation's critical infrastructure, the EIS-GCC was one of the first developments of that designation. The EIS-GCC is a first of its kind collaboration among federal, state, and local officials to secure elections, working to formalize and improve information-sharing and communication protocols to ensure that timely threat information, support, and resources reach all election officials so they can respond to threats as they emerge. The EIS-GCC has 29 members, of which 24 are state and local election officials. It also includes members from the U.S. Department of Homeland Security (DHS), the U.S. Election Assistance Commission, the National Association of State Election Directors (NASED), the Election Center, and the International Association of Government Officials. The members of the EIS-GCC are working to update an elections-sector specific plan, improve communications protocols and portals, and secure increased resources for state and local election officials. In addition to the GCC, a Sector Coordinating Council (SCC) was also established for non-government, private sector entities to better communicate with election officials and the federal government.

Beyond the EIS-GCC, DHS and the Center for Internet Security (CIS) have been particularly strong partners. Pennsylvania and other states regularly collaborate with DHS on independent risk and vulnerability assessments, intelligence, training, tabletop exercises, communications,

and more. We also work with CIS's Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure Information Sharing and Analysis Center, (EI-ISAC) to gather and share intelligence about cyber threats that target government or government-affiliated systems, and gain support and resources including forensic analyses and emergency response assistance. Additionally, the cyber defense team of the Pennsylvania National Guard has been an exceptionally strong partner. Within the last year they were the first National Guard team selected to participate in a new DHS program, to be trained to conduct Risk and Vulnerability Assessments to DHS standards.

For all these strong collaborative partnerships to be most effective, and for additional goals to be advanced, more resources are needed. Some top priorities would include the federal government playing a greater role with vendor oversight, including tracking vendor foreign ownership, data hosting, manufacturing and employee background checks, and chain of custody for all voting and election system components; and reinforcing Continuity of Operations Plans (COOP) across levels and sectors, to provide more clarity on primary points of contact in the federal government for incidents and concerns. It would also be beneficial to have broader communications between our federal election security partners and our state legislatures and counties, so that counties and legislators could hear directly about federal election security priorities and concerns. We also need to strengthen lines of communication from the federal government to the state chief election officials, for example to ensure that federal entities notify the state when local incidents are reported, so that we may immediately act when necessary. Additionally, federal funding and support are needed to ensure that all counties have state-of-the-art intrusion detection systems, comprehensive phishing, cyber hygiene, and security awareness training, vulnerability assessments, and more.

PENNSYLVANIA LANDSCAPE

Most people have an understanding that the word "cyber" relates to the study of systems and the intersections and communications between people and machines. But the word "cyber" actually has ancient Greek origins, deriving from the Greek word for the "gift of governance" and "leadership." In Pennsylvania, we have been tapping both aspects of the word in our election security planning, using resilient and integrated governance and leadership to enhance the intersections and communications between people and machines, to continue to advance our technologies while also doing so in a way that protects our democracy and develops collaborative and responsive policy and leadership. This requires a tremendous amount of resources but has immeasurable value.

Collaboration

Thanks to Governor Wolf's deep commitment, we have employed a multi-layered and cross-sector security strategy to election security. We broke down silos and brought together experts from multiple fields and sectors at the local, state, and federal levels, including professionals in information technology, law enforcement, homeland security, defense, elections, and emergency preparedness. Beginning in 2018, we formed an executive Interagency Workgroup on Election

Security and Preparedness, banding together experts from the Department of State (DOS), Homeland Security, Emergency Management Agency, Information Technology, State Police, National Guard, the Inspector General, and the Department of Military and Veterans Affairs. This team of key agencies meets regularly and collaborates on increasing election security training, support, assessment, information, and preparedness, to implement best practices to respond to and mitigate continuously evolving security threats.

We also formed a county/state election security workgroup of County Commissioners Association of Pennsylvania (CCAP), county election directors, DOS staff, and county and state CIOs and IT personnel. This workgroup discusses security issues and shares training resources, including guidance, security awareness training, and resources on strong cyber security practices for voting system and network preparation and security, including pre-election testing, password and permissions management, restricting access, file transfers, and vote canvassing. We are also providing anti-phishing and security training tools to all 67 counties at no cost to them.

We have collaborated with all these state and federal partners to provide tabletop exercises to counties and partners, modeled after common military and law enforcement techniques, to train election, information technology, and security personnel in incident response and preparation, simulating scenarios that could impact voting operations.

We were the first state in the nation to accept DHS's offer to provide vulnerability assessments to the states – we did this in 2016, 2018, and are planning a third assessment in the next several months. We have tools in place to identify vulnerabilities, detect network intrusion, and encrypt data in-transit and at rest. We engage in ongoing continuity and disaster recovery exercises and review and revise as necessary our COOP plans several times each year.

Voting System Upgrades and Post-Election Audits

As of 2018, Pennsylvania was one of the small minority of states still primarily voting on paperless Direct Recording Electronic (DRE) voting systems. In April 2018, DOS directed all 67 counties to purchase new voting systems that meet current security and accessibility standards, and which include a voter-verifiable paper record with plain text language that voters can verify before casting their ballot and that local officials can use in recounts and post-election audits. These new systems must be in use no later than by the primary of 2020, and preferably by the November 2019 election.

In order to bolster our voting system security even further, in 2018 DOS created new security standards by which to evaluate the new voting systems applying for certification in PA. PA law requires both federal and state certification, and because the federal EAC had not updated its standards in some time and did not have a quorum to do so at the time, we decided to update our state security standards, and additionally assess the accessibility of the systems. The new voting system standards incorporated tests to ensure confidentiality, vote anonymity, integrity, security, auditability, and usability of the voting systems. All new certified systems in Pennsylvania have passed the following tests:

- Penetration testing that evaluates the security of the voting system by trying to exploit potential vulnerabilities.
- Access control testing to confirm that the voting system can detect and prevent unauthorized access to the system and election data.
- Evaluation of voting system audit logging capabilities to confirm that the system logs will allow auditing, as well as investigation of any apparent fraudulent or malicious activity.
- Tests that ensure every physical access point is well secured and system software and firmware is protected from tampering.

To evaluate accessibility of voting systems for voters with disabilities, we utilized expert review by usability and accessibility examiners as well as feedback from voters with disabilities and poll workers.

DOS has certified seven new voting systems that meet these standards, and we are very pleased with the remarkable progress made by the counties. The county election directors and commissioners have been incredibly dedicated to acquiring voting systems that best meet their voters' needs and provide the most secure, auditable, and accessible voting systems to all Pennsylvanians. Already, 75 percent of counties have officially voted to select new systems, and 46 out of 67 counties are utilizing their new systems with verifiable paper records in November 2019. The remaining counties are still hard at work planning and evaluating their voting system choices, reviewing vendor quotes and prices, holding new voting system demonstrations for the public, consulting with voters and poll workers and exploring funding and financing options.

Cost, of course, remains a major concern for counties. Since the beginning of this initiative, we have been committed to this enterprise being a cost-share of federal, state, and local dollars. Toward this end, we designated 100% of the federal funds appropriated in 2018 for election security proportionately to the counties for replacement of their voting systems by 2020, totaling $14.15 million in PA (including a 5% state match). Though a welcome down payment and approximately 10-12% of the total costs of the new systems, $14.15 million is not nearly enough, and we are pursuing additional state and federal funding.

We have also formed a statewide post-election audit working group, which includes election officials from six counties of different sizes and demographics across the state, as well as expert advisors on audits and elections. This working group is studying audit models such as risk-limiting audits and is developing best practice recommendations for post-election audits that will review the plain text on the paper records and the tabulated votes to confirm to a reasonable degree of statistical certainty the accuracy of the outcome of the election.

The dedication and thorough examination by the members of this workgroup to developing effective models has been inspirational and should be a model for other states looking to explore these practices. In addition, two of our counties on opposite sides of the state, Philadelphia and Mercer county, have volunteered to pilot advanced post-election audits this November 2019,

which will offer confidence to the voters as well as the opportunity to establish and test real-time best practices. Additional Pennsylvania counties will also be piloting audits over the next several years, and we expect all counties to employ enhanced audits by the 2022 general election.

Looking Forward

Looking forward, we continue to build. The above initiatives have taken and will continue to take significant resources to advance. In addition to advancing and strengthening all of the above, our highest priority goals and need for additional resources include: replacing our statewide voter registration system (SURE); ensuring all counties have advanced intrusion detection systems and practices, ongoing and evolving comprehensive cyber hygiene assessments, COOP and security training, and vulnerability assessments; and implementing new voting systems, strengthened pre-election testing, and enhanced post-election audits statewide.

CONCLUSION

On Election Day 2018, we saw what happens when all of the collaboration and hard work comes to fruition, and the powerful benefits of the intersection of all of the above in action. We were connected throughout the day to the counties, state agencies, other states, and the federal government through shared dashboards and frequent communications. For example, if another state was seeing attempted attacks coming from particular IP addresses, they were able to share with other states, allowing us to block those IP addresses at the state level, and then Pennsylvania would share those IP addresses with all 67 counties to enable them to block those IP addresses as well. We had conference calls throughout the day with our interagency group members and counties, sharing what we were hearing and seeing, any concerns, and any support or resolutions we could provide from our different sectors. This collaboration and communication allowed us to be proactive in our defenses, rather than just reactive as might have occurred in the past.

The right to vote is a fundamental right, and every voter must be provided equal access to the polls and deep-seated confidence in the security and accuracy of their vote. We cannot allow circumstances to develop whereby voters in under-resourced counties have less security or less accessibility in their vote. Pennsylvania — where both the Declaration of Independence and the U.S. Constitution were adopted — takes its legacy as the birthplace of American democracy very seriously, and we know that the foundation of that democracy rests on the security, auditability, accessibility and integrity of our elections. We urge you please to invest additional funds to ensure this for ourselves and for generations to come. Our democracy - and bolstering voters' confidence in their ability to participate fully in that democracy - is worth every dollar.

Thank you for the opportunity to testify on this important issue, and I am happy to answer any questions you may have.

Auditor's Conclusion to the Department of State's Response

Note: The page numbers referred to by the Department of State (DOS) in its response are from a draft report of the findings and recommendations and do not correspond to the page numbers in this final report; therefore, in this conclusion, we will refer to the respective findings and subsections in this report as necessary.

Overall, we are highly discouraged not only by management's responses to our draft findings, but also the general negative tone of the response. This is particularly surprising since the DOS itself requested the audit and the Department of the Auditor General (DAG) made every possible effort to provide a cooperative and constructive auditing process DAG takes exception to DOS' multiple mischaracterizations and flawed arguments. Additionally, DOS did not provide specific examples to us to prove that our analysis of the data was incorrect.

More general comments are below:

We are concerned that DOS' efforts to deflect recognized weaknesses in the SURE system will inhibit its ability to recognize existing shortfalls and improve the SURE system overall. Additionally, we were exceedingly surprised that DOS' response indicates that it strongly disagrees with many of our findings and it completely mischaracterizes information that was provided, or not provided to us in many instances, during the course of our audit. In its attempt to discredit our findings, DOS does not seem to understand that a primary objective of our audit was to assess the accuracy of records maintained in the SURE system. Our audit procedures disclosed internal control weaknesses related to input and maintenance of voter records. Our data analysis revealed examples of potential inaccuracies, all of which should be properly investigated by forwarding the information to the counties for further examination. Tests of accuracy are performed by comparing data to other sources, searching for duplicate information, and checking for inconsistencies and unreasonable values. In one example, DOS appears to assume that because a middle initial is different between two records, then the records are definitively those of different persons despite two or more other personal elements (e.g. date of birth (DOB), last four digits of Social Security number) being exactly the same. We disagree. In light of the internal control weaknesses found, there is potential in this example, that a data entry error could have occurred when typing the middle initial, which is why we continue to recommend that these cases warrant further investigation. We are concerned that DOS, and therefore the counties, will not utilize the information provided to them in the audit because it is assuming that the data in the SURE system is accurate. Our data analysis and internal control assessment strongly suggest otherwise.

Further, while DOS requested this audit, its management does not seem to grasp that we cannot properly conclude and satisfy the audit objectives in accordance with generally accepted *Government Auditing Standards* without obtaining sufficient, appropriate evidence. Yet, in spite of the limitations imposed by DOS, we believe we have provided DOS with recommendations

that, if appropriately implemented, will improve the security of Pennsylvania's voter registration system and the completeness, accuracy, and auditability of its voter registration records.

A large portion of DOS management's comments appears to be an attempt to deflect their uncooperativeness and shortcomings. While DOS spent considerable effort noting how they were not provided sufficient time to respond to our audit report, they failed to acknowledge that per the Interagency Agreement, effective May 15, 2018, the audit was due to be released no later than January 31, 2019. In fact, the Interagency Agreement specifically sought to eliminate any potential timing conflicts with the November 2019 election when it set the release date of January 31, 2019. While DOS agreed to such terms in the Interagency Agreement, they nevertheless failed to follow its spirit and now seek to discredit DAG's overwhelming attempts to accommodate DOS. This deadline was postponed three times due solely to DOS' inability to provide DAG with timely responses. Had DOS cooperated and provided DAG with timely responses to our requests, the report would have been issued as agreed upon, and therefore would not have interfered with the November 2019 election. Contrary to DOS' comments, DAG does not believe that our report is more important than the election; however, we too have a responsibility to deliver, in a timely manner, quality audits to the taxpayers of Pennsylvania.

DOS provided information throughout its response regarding updates and events that have occurred or procedures that have been implemented since the end of our audit procedures on April 16, 2019. As we have not performed a review of all of these events or procedures, we cannot comment regarding these items. We did confirm certain updated information provided regarding the *Introduction and Background* and incorporated this new information into our report. We also appreciate DOS' comments supportive of our results for certain work performed.

The following sections provide clarification regarding DOS' responses to specific information related to our findings and certain background information included in this report.

Finding 1 - As a result of the Department of State's denial of access to critical documents and excessive redaction of documentation, the Department of the Auditor General was severely restricted from meeting its audit objectives in an audit which the Department of State itself had requested.

DOS refutes *Finding 1* and maintains its decision to not provide certain information. DOS further suggests there was a misunderstanding as to our audit objective to review security protocols of the SURE system and believes it provided us with enough evidence to satisfy this objective. We strongly disagree with DOS' response, and in particular, regarding DOS' statement that DAG acknowledged that it had a lack of expertise and the knowledge to conduct a substantive security audit. When DAG was approached concerning a possible audit of the voter registration system, we realized that cybersecurity would be a significant part of the audit. Our IT Audit Managers are all Certified Information Systems Auditors and receive training on cybersecurity. We acknowledged, however, that we had insufficient resources in-house

specifically to perform network penetration testing. Also known as "ethical hacking," penetration testing attempts to locate vulnerabilities in a computer system by breaking into it using the same tools as malicious cyber criminals. While we have observed penetration tests performed by other auditors, we did not have the expertise in-house to hack systems and expressed that fact.

During a preliminary discussion, officials from the Office of Administration, Office for Information Technology (OA/OIT), explained that appropriate network penetration testing had already been performed and we could rely on that testing. We agreed that we would most likely be able to rely on the work performed by other auditors in this area if we could review the reports. We explained that we would require access to the network penetration audit reports since *Government Auditing Standards* require us to consider the work of other auditors and to determine the status of corrective actions.[116] With assurances received that we would have access to the reports, we recommended acceptance of the engagement.

We were therefore, very surprised in July 2018 when access to the reports was abruptly denied on the very day we were scheduled to review the reports. We were surprised again when we attempted to perform our own IT controls testing, both in the area of cybersecurity and the more routine IT general controls, and found that DOS delayed, blocked, or redacted information required to complete the audit in accordance with *Government Auditing Standards*. We explained that assessment of the effectiveness of Information System controls (also referred to as IT controls) was required by *Government Auditing Standards* because IT was so significant to multiple audit objectives including controls over adding and maintaining voter records.[117] While DOS provided verbal and written representations as to the level of controls in place, testimonial evidence alone is not considered sufficient evidence on which to base an audit.[118] Further, hundreds (if not thousands) of pages of reports with the entire contents redacted from top to bottom provides no evidence of scope, results, or corrective actions.[119] We were, therefore, not able to obtain sufficient evidence to comply fully with *Government Auditing Standards* in this area as stated (see *Scope Limitation A* in *Finding 1*).

DOS provided a letter from the *Pennsylvania Interagency Election Security and Preparedness Workgroup* dated October 28, 2019, long after completion of our audit procedures and seven-and-a-half months after a deadline to receive documentation for the audit, supporting DOS' decision not to provide reports and documentation needed to complete the audit (DOS' Exhibit A). As noted in *Finding 1*, however, the Auditor General traveled to Washington D.C. to meet with representatives from the U.S. Department of Homeland Security who stated that sharing Homeland Security reports was left up to the discretion of each particular state. Further, our consultations with cybersecurity audit experts from other state audit organizations during the audit confirmed our absolute need to review these outside reports in order to comply with *Government Auditing Standards*. Experts from the University of Pittsburgh Institute for Cyber

[116] U.S. Government Accountability Office. *Government Auditing Standards.* 2011 Revision. Paragraph 6.62.
[117] Ibid., Paragraph 6.16.
[118] Ibid., Paragraph 6.62.
[119] Ibid., Paragraph 6.36

Law, Policy and Security, in *The Blue Ribbon Commission on Pennsylvania's Election Security: Study and Recommendations* recommended that DOS cooperate fully with the Pennsylvania Auditor General's audit and recommended specifically that the DAG examine cyber incident response plans. In fact, the report states, *"…it should not be problematic to share sensitive information about cyber incident response plans with those officials."*[120] Finally, it should be noted that the cyber security reports we had attempted to review for purposes of this audit were, prior to our request, available to numerous individuals, including non-DOS employees, who had access to these documents. Although we were told that we could not be provided with these reports because of "DOS policy," no such policy existed until April of 2019, after our deadline to submit documentation for the audit. DOS was unable to determine which individuals who had access to these reports actually viewed, copied or circulated them. This systemic behavior is concerning because it evidences a lack of established, well thought-out, and enforced policy until DAG requested access to documents, which apparently were provided freely to non DAG employees prior to our audit.

Regarding DOS' response related to information provided by the Pennsylvania Department of Transportation (PennDOT), we acknowledge in *Finding 6* that PennDOT provided us with limited documentation, but it did not contain all the Motor Voter information needed to complete our assessment of whether records maintained within the SURE system are accurate and in accordance with the Help America Vote Act (HAVA) and Pennsylvania law. As DOS indicates in its response, the information provided was in the form of an Excel spreadsheet rather than directly from the data source. Since information can easily be manipulated in Excel, we could not conclude that the data provided was reliable, and therefore, we could not use it for testing purposes. Screen shots provided information regarding the voters' driver's license information but did not contain all the fields of information that we were testing for voter registration such as political party and residence versus mailing address, which could be different as in the case of college students.

Further, DOS is inaccurate in their response that the report states that DOS does not maintain source documentation for Motor Voter applications. We did not request Motor Voter information from DOS since PennDOT, not DOS, is the original recipient of Motor Voter applications. Additionally, although DOS contends that they have source data for Online Voter Registration applications, when we requested that information on January 30, 2019, while at the DOS offices conducting testing, we were verbally informed that there was nothing available for us to review. Although DOS contends that the data is stored in multiple locations within the SURE architecture, the data was not provided to us when requested.

Regarding DOS' delay in responding to our requests for information, we agree that some of the requested information would take longer than the standard three business days to compile. Due

[120] The University of Pittsburgh Institute for Cyber Law, Policy and Security. *The Blue Ribbon Commission on Pennsylvania's Election Security: Study and Recommendations*, January 4, 2019. Pages 10, 37, 38, and 53. https://www.cyber.pitt.edu/sites/default/files/FINAL%20FULL%20PittCyber_PAs_Election_Security_Report_0.pdf

to this fact, we informed DOS at the beginning of the audit that if they anticipated needing additional time, they could notify us in writing of that request so that we would be aware of the delay. As we noted in *Finding 1*, DOS only requested an extension one time. Although we did submit requests for information during DOS identified blackout periods, this was done to allow for the continuation of the audit after much delay by DOS. As previously stated, we had informed DOS that if additional time was needed to please notify us, which DOS chose not to do. Further, DOS identified multiple blackout periods some of which only affected certain DOS offices or county election offices. As we could not be sure which offices were impacted during the blackout dates, we submitted requests for information, again with the understanding that DOS could notify us if an extension was needed to provide the requested information. Although DOS contends that its staff regularly communicated to DAG the status of outstanding requests, the only response that DAG received from DOS was DOS' acknowledgment that the information requests had been received, that they would review the request and "be in touch," or that staff were working on the requests without providing any detail as to when or if the information would be provided to DAG.

DOS stated in its response that the Request for Proposals (RFP) for the new voter registration system to replace the current SURE system has been completed. We are encouraged that based on a cursory review of the RFP posted on October 9, 2019, it appears that DOS has included certain edit checks and other application controls recommended in our report and preliminarily discussed with DOS management on August 19, 2019. Our recommendations included the use of driver's license numbers in the search for duplicates, the incorporation of Geographic Information System (GIS) capability, and the expansion of the use of data available from the Electronic Registration Information Center (ERIC). We believe this will help reduce errors and inaccuracies when processing voter applications and performing subsequent list maintenance.

Finding 2 – Data analysis identified tens of thousands of potential duplicate and inaccurate voter records, as well as voter records for nearly three thousand potentially deceased voters that had not been removed from the SURE system.

Finding 2 describes the results of our data analysis that DOS requested in the Interagency Agreement to conduct our audit. Due to audit time, financial, and staffing constraints, we did not validate the thousands of cases/situations identified, and as a result, we use the term "potential" to be conservative. We believe, however, that in most of these instances, there are inaccuracies within the data maintained in SURE, and therefore, DOS needs to work with the counties to properly investigate and address <u>all</u> of these situations and correct the voter records as appropriate to ensure that SURE contains accurate information, as required by law. We are concerned that by dismissing specific potential errors noted in the findings, DOS is missing the larger issue that inaccurate data exists in SURE and that they will not properly forward the information to counties to investigate and correct the data, if necessary.

Of note, DOS does not comment on the 24,408 cases where the same DL number is listed in more than one voter record, which appears to be an indication that the data analysis yielded results that will be helpful for improving the accuracy of the data, and that DOS agrees that some of the information in SURE is not accurate. As for the 13,913 other potential duplicate cases, DOS focuses on one subset of 1,612 potential duplicate records and accuses DAG of inaccurate analysis. DOS is assuming, however, the data is accurate stating that because a middle initial may be different between two records, a duplicate does not exist even though the first name, last name, and last four digits of the social security number are the same. DOS is assuming the difference in middle initials is always accurate and states those cases need no further investigation. The complacency of DOS in a matter of such importance is, in a word, disheartening. We wholly disagree in that our report provides examples of many instances where data in the SURE system certainly appears inaccurate. DOS should forward all of the cases and related information to the counties to investigate and determine whether the data is correct or whether a duplicate exists.

DOS claims to have disproved "multiple allegations". Despite DOS' assertion that certain data analysis was flawed, DOS provided no specific examples to us to prove that our analysis of the data was incorrect. As a result, our data analysis stands and we continue to recommend that DOS forward the detailed exceptions to the counties for investigation.

In its response, DOS mischaracterizes data we provided regarding the results of our analysis. To clarify, DAG provided detailed files of each exception noted in the report on October 1, 2019. These files were in Microsoft Excel format and each file included the programming logic that we used in our data analysis software, ACL, to extract the exceptions. On October 8, 2019, DOS requested copies of the entire database used in our analysis. On October 9, 2019, DAG provided copies of the raw data provided by DOS in 2018 in the exact same format as we had received it from DOS. Since it is an exact copy of their own data, we are confused as to why DOS expressed difficulty with its own data format.

DOS maintains that the delay in providing the data files in 2018 was due to the negotiation of a Non-Disclosure Agreement (NDA) with ERIC that occurred over the course of approximately three months. DAG documentation, however, indicates that the DAG received the NDA from DOS on August 7, 2018. DAG reviewed and signed the NDA to DOS on August 15, 2018, or eight days later. DOS did not provide the data until an additional 56 days passed on October 10, 2018. Therefore, we disagree with DOS that the delay was due to the NDA.

DOS expressed concerns about not receiving extensions to investigate the exceptions prior to release of the report and that the deadline for their response would be prior to Election Day. DOS, however, agreed to the response timeline prior to DAG providing management the draft report. Additionally, DAG immediately agreed to an additional one-week extension requested by DOS upon their receipt of the draft report. Therefore, DOS management was fully aware and agreed that its response would be prior to the election. Further, throughout the audit DAG agreed to numerous extensions to the sole benefit of DOS such that the release of this report has been

delayed nearly a full year after the original release date agreed upon in the Interagency Agreement. If we had agreed to further extensions to the audit timeline, there would be insufficient time for the counties to investigate the potential data exceptions and correct them prior to the next Presidential general election. As it is, the counties have less than one year until that election to obtain the exceptions, investigate them, and correct the records, if necessary. We recommend DOS provide the detailed exceptions to the counties as soon as possible to give them more time to validate their data or make corrections as appropriate.

Concerning potential DOB inaccuracies identified by DAG, DOS maintained that some of the records that were identified as erroneous DOB are in fact correct. For instance, they noted that county election officials must comply with the Sexual Violence Victim Address Confidentiality Act that requires county election officials to list a generic DOB in the SURE system to safeguard personal information. DOS informed us of its use of generic DOB when transitioning to the current SURE system; however, it did not provide us any information during the audit regarding the need to use generic DOB to comply with requirements to maintain confidential information of the victims of sexual violence. Therefore, the findings and results of our DOB inaccuracies analysis will remain as written in the revised draft report.

Finding 3 - The Department of State must implement leading information technology security practices and information technology general controls to protect the SURE system and ensure the reliability of voter registration records.

DOS contends that the SURE Advisory Board performs the functions of an oversight body. The Board's charter, however, only allows it to function in an advisory capacity rather than as an IT governance body responsible for ensuring effective IT management. Further, in light of Executive Order 2016-06, OA/OIT and the Employment, Banking, and Revenue (EBR) Delivery Center should have direct representation on the IT governance oversight body.[121] DOS' response notes that the Chief Information Officer for the EBR Delivery Center holds regular steering committee meetings with DOS; however, this committee does not have a formal charter. An IT governance oversight body's charter should include all the key areas of IT governance such as value delivery, strategic alignment, resource management, risk management, and performance management.[122]

We are encouraged by DOS' efforts to modify its vendor's IT support and maintenance services as described in its management response. We are also pleased that our audit results in this area have been helpful.

[121] Executive Order 2016-06, *Enterprise information Technology Governance*, dated April 18, 2016.
[122] Information Systems Audit and Control Association (ISACA). http://www.isaca.org/chapters9/Accra/Events/Documents/ISACA%20Presentation%20-%20IT%20Governance%20V5.pdf. (accessed December 5, 2019).

Although DOS states in its response that vendors are already monitored in accordance with Management Directive 325.13, DOS provided no evidence that this monitoring was actually performed. As stewards of election infrastructure, DOS cannot simply rely on other agencies and their vendors to ensure voter data is secure. We continue to recommend that DOS: (1) ensure agreements with other agencies require that vendors comply with policy; (2) monitor System and Organization Control reports of all vendors key to election infrastructure (EI); and (3) coordinate with PennDOT and OA/OIT to ensure their vendor oversight practices contribute to EI security.

We are pleased that DOS is updating its *Equipment Use Policy* and is planning to have all appropriate SURE users sign the updated policy. We found, however, that the section of the policy on the use of county-owned equipment to be less strongly worded than other sections of the policy and continue to recommend that DOS revise the policy to clearly address the risks of connecting county-owned equipment to SURE. We agree that instituting the use of a form to formalize county configuration requests and organizing county-level policies will help to encourage compliance.

Finding 4 - Voter record information is inaccurate due to weaknesses in the voter registration application process and the maintenance of voter records in the SURE system.

Although DOS strongly disagrees that there are significant weaknesses in the voter registration process, DOS agreed that edit checks are warranted. Edit checks help to ensure the accuracy of data obtained during the voter registration process. DOS further states that it has already implemented some of the recommendations to improve the application process and intends to do a thorough data analysis prior to moving to a new system so that they are starting with the most accurate data possible. We are confused as to why DOS would state that it disagrees that there are significant weaknesses but then also states that they have made and intend to make additional improvements to the process.

DOS disagrees with the recommendation related to rejecting voter registration applications in a pending status for non-match of information. DAG's recommendation, however, was for DOS to determine if it can direct the counties to review their pending applications and process them (either approve or reject), and to establish a maximum amount of time in which an application can remain in pending status before the county either approves or rejects the application. The recommendation did not indicate that applications pending due to a non-match of information be rejected. It is DAG's stance that an application that has been in pending status for months or even years is a disservice to the applicant. Long-term pending applications should be cleaned up prior to migrating to the new system so not to carry unneeded/outdated data into the new system.

Regarding the recommendations made for the remaining areas in *Finding 4*, we are pleased to see that DOS will take them under advisement. We hope that ultimately DOS implements our recommendations to ensure improvements to its processes.

Finding 5 - Incorporating edit checks and other improvements into the design of the replacement system for SURE will reduce data errors and improve accuracy.

Although DOS indicated that the SURE system is designed to automatically associate the proper voter registration record cancellation reason with the source of the cancellation transaction, this does not address the issue we identified for voter registrations that may have been improperly cancelled within 90 days of an election. We welcome DOS' response that it intends to review the data analysis in the coming weeks and will follow up with counties as necessary. A significant purpose of our review was to identify potential data errors and share that information with DOS and the counties so that they could investigate and correct erroneous information, if applicable.

Finding 6 - A combination of a lack of cooperation by certain county election offices and PennDOT, as well as source documents not being available for seventy percent of our test sample, resulted in our inability to form any conclusions as to the accuracy of the entire population of voter records maintained in the SURE system.

We have already addressed in the *Finding 1* portion of this section the issues that DOS takes in its response regarding the lack of source documentation, and are pleased that DOS intends to take our recommendations under advisement regarding the retention of records policy and scanning documents.

Finding 7 - The Department of State should update current job aids and develop additional job aids and guidance to address issues such as duplicate voter records, records of potentially deceased voters on the voter rolls, pending applications, and records retention.

We are most pleased to see that DOS agrees with our recommendations and/or plans to review the job aids and discuss our recommendations with appropriate individuals regarding implementation.

Appendix D

Regarding DOS' comments about the Commonwealth's voter registration process addressed in *Appendix D* of our report, DOS took issue with DAG's statement that DOS and the counties must continue to address the concern with the PennDOT Motor Voter system that allowed ineligible individuals to register to vote. We understand that DOS has shared the information with the counties to take further action; however, we emphasize the vital importance that DOS should continue to follow through and work with the counties to ensure that this work is performed for those voters identified as potentially ineligible voters.

Appendix A | Objectives, Scope, and Methodology

The Department of the Auditor General (DAG) conducted this performance audit pursuant to an Interagency Agreement (agreement) entered into by and between the Department of State (DOS) and DAG to assess DOS' administration of the Statewide Uniform Registry of Electors (SURE).[123] We also conducted this audit under the authority of Sections 402 and 403 of The Fiscal Code, 72 P.S. §§ 402 and 403.

We conducted this audit in accordance with applicable *Government Auditing Standards*, issued by the Comptroller General of the United States, except for certain applicable requirements that were not followed. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.[124] Significant scope limitations caused by a lack of cooperation from DOS, the Pennsylvania Department of Transportation (PennDOT), and certain county election offices (counties), as well as a failure to provide the necessary information, affected our ability to obtain sufficient, appropriate evidence to fully achieve all of the audit objectives as described below and within *Finding 1*.

Objectives

The agreement specifies the following audit objectives:

1. Assessment of whether records maintained within the SURE system are accurate and in accordance with the Help America Vote Act (HAVA) and Pennsylvania law. [See *Findings 2, 4, 5, 6*]
2. Evaluation of the process for input and maintenance of voter registration records. [See *Finding 4*]
3. Review of security protocols of the SURE system. [See *Findings 1, 3*]
4. Review of the efficiency and accuracy of the SURE system. [See *Finding 5*]
5. Review of the internal controls, methodology for internal audits and internal audits review process. [See *Finding 4*]
6. Review of the external controls, methodology for external audits and external audits review process. [See *Finding 1*]
7. Review of the methodology for the issuance of directives and guidance to the counties by DOS regarding voter registration and list maintenance. [See *Finding 7*]

[123] See *Appendix B* for a copy of the Interagency Agreement.
[124] U.S. Government Accountability Office. *Government Auditing Standards*. 2011 Revision. Standards related to obtaining sufficient, appropriate evidence are included in Paragraphs 6.56 through 6.72, standards related to obtaining an understanding of information system controls are included in Paragraphs 6.23 through 6.27, and standards related to review of previous audits and attestation engagements are included in Paragraph 6.36.

8. Any other relevant information or recommendations related to the accuracy, operability, and efficiency of the SURE system, as determined by the Auditor General. [No Findings]

Scope

This performance audit covered the period January 1, 2016 through April 16, 2019, unless otherwise noted, with updates through the report date.

DOS management is responsible for establishing and maintaining effective internal controls to provide reasonable assurance of compliance with applicable laws and regulations, contracts, grant agreements, and administrative policies and procedures. In conducting our audit, we obtained an understanding of DOS' internal controls, including information systems controls, where possible given the scope limitations placed on the audit that we considered to be significant within the context of our audit objectives.

For those internal controls that we determined to be significant within the context of our audit objectives, including information system controls where possible given the scope limitations, we also assessed the effectiveness of the design and implementation of those controls as discussed in the *Methodology* section that follows. Deficiencies in internal controls that we identified during the conduct of our audit and determined to be significant within the context of our audit objectives are included within the respective audit findings in this report. In addition, during our procedures we identified areas of potential improvement related to computer security, information technology general controls, and interface controls that we have specifically excluded from this report because of the sensitive nature of this information. These conditions and our recommendations have been included in a separate, confidential communication to DOS management.

Government Auditing Standards require that we consider information systems controls "…to obtain sufficient, appropriate evidence to support the audit findings and conclusions."[125] This process also involves determining whether the data that supports the audit objectives is reliable. In addition, Publication GAO-09-680G, *Assessing the Reliability of Computer-Processed Data*, provides guidance for evaluating data using various tests of sufficiency and appropriateness when the data are integral to the audit objective(s).[126] We attempted, where possible despite the scope limitations, to comply with standards concerning the reliability of computer-processed data. See our assessment in the *Data Reliability* section that follows.

[125] U.S. Government Accountability Office. *Government Auditing Standards*. 2011 Revision. Paragraphs 6.23 through 6.27.
[126] U.S. Government Accountability Office. *Assessing the Reliability of Computer-Processed Data*, July 2009.

Scope Limitations

Due to a lack of cooperation from DOS, the Pennsylvania Department of Transportation (PennDOT), and certain county election offices (counties), as well as a failure to provide the necessary information needed to satisfy three of eight audit objectives, it became evident that DAG would not be able to perform the audit in accordance with certain applicable standards in *Government Auditing Standards*, which is issued by the U.S. Government Accountability Office. The standards in question include obtaining sufficient, appropriate evidence; evaluating the design and operating effectiveness of information systems controls; and reviewing previous audits and attestation engagements significant within the context of the audit objectives.[127] DAG issued a modified *Government Auditing Standards* compliance statement for this audit to account for the significant scope limitations that resulted from DOS' refusal to provide access to documentation and data required to complete the audit. See these scope limitations addressed in detail in *Finding 1* of this report and summarized below.

Due to a lack of source documentation to support voter registration applications (applications) filed online and through paper forms and PennDOT's refusal to provide access to source documentation for Motor Voter registration applications, we were unable to determine if the records within the SURE system are accurate. We were, therefore, unable to satisfy our audit objective to perform a sufficient assessment of whether records maintained within the SURE system are accurate and in accordance with HAVA and Pennsylvania law (Objective 1).

Further, DOS' refusal to provide sufficient access to key documentation related to the security and operation of the SURE system significantly limited our ability to perform our audit procedures. The following list identifies the key documents/information that were not provided (items 1, 2, and 5) or were heavily redacted (items 3 and 4):

1. Contents of external security assessment reports issued by the United States Department of Homeland Security (Homeland Security), as well as reports issued by private firms contracted to assess security.

2. Systems and Organization Control reports detailing the security practices in place at outside vendors key to the security and operation of the SURE system.[128]

3. Detailed information on system configuration and implementation of cybersecurity policies.

[127] U.S. Government Accountability Office. *Government Auditing Standards*. 2011 Revision. Standards related to obtaining sufficient appropriate evidence are included in Paragraphs 6.56 through 6.72, standards related to obtaining an understanding of information system controls are included in Paragraphs 6.23 through 6.27, and standards related to review of previous audits and attestation engagements are included in Paragraph 6.36.
[128] Systems and Organization Control (SOC) reports are reports on a service organization's controls by an independent auditor.

4. The formal results and corrective action plans from the 2018 test of the emergency recovery system.

5. Documentation of significant IT controls and system interfaces.

Without these critical documents listed above, we were unable to satisfy our audit objective to review the security protocols of the SURE system (Objective 3). In addition, we were unable to comply with *Government Auditing Standards*, which requires auditors to evaluate the design and operating effectiveness of information systems controls and review previous audits and assessments significant within the context of our audit objectives.[129] DOS' refusal to provide these documents resulted in our inability to provide a conclusion regarding the security of the SURE system. Additionally, as a result of not being provided access to the contents of the external security assessment reports, we were not able to determine what these assessments included and therefore, have no assurance that the assessments covered all of the various layers of security protecting the SURE system (Objective 6).

Methodology

Items selected for testing within this audit were based on various methods including statistical sampling and auditor's professional judgment. Due to the scope limitations regarding our testing of the statistical sample, we were not able to project results to the corresponding population. For our other test selections using professional judgment, the results of our testing also cannot be projected to, and are not representative of, the corresponding populations.

To address the audit objectives, we performed the following procedures:

- Interviewed and corresponded with individuals from the following offices to gain an understanding of SURE and security protocols of the SURE system, the individuals involved in managing, maintaining, and monitoring work performed in SURE, the assistance provided when requested by those utilizing SURE, and work performed regarding the issue with non-citizens that had the ability to register to vote at PennDOT photo license centers:

    - DOS management, staff, information technology officials, and legal counsel
    - SURE Help Desk staff
    - County election offices (county) management and staff
    - PennDOT management, staff, and legal counsel

[129] U.S. Government Accountability Office. *Government Auditing Standards*. 2011 Revision. Paragraph 6.23 through 6.27.

- Reviewed the following laws, regulations, contracts, and written policies and procedures applicable to SURE:

  - Help America Vote Act of 2002, 52 U.S.C. § 21083 regarding the requirement to implement a computerized statewide voter registration list, minimum standards for the accuracy of voter registration records and requirements regarding performing list maintenance on a regular basis to remove ineligible voters.
  - National Voter Registration Act, 52 U.S.C. § 20507 regarding the federal requirements to register to vote.
  - Pennsylvania Voter Registration Law (Act 3 of 2002), 25 Pa.C.S. Chapters 12 and 19 regarding the implementation of HAVA in state law.
  - 4 Pa. Code Chapter 183 regarding record retention guidance on applications.
  - *County Records Manual* issued by the Pennsylvania Historical and Museum Commission regarding record retention guidance on applications.
  - SURE job aids, created and distributed by DOS to the counties, that provide guidance regarding the current process established in the SURE system. In particular those processes regarding processing applications, including pending applications, and list maintenance performed on voter registration records.
  - DOS' Memoranda of Understanding with both PennDOT and the Department of Health (DOH) for systems that interface with the SURE system.
  - DOS' contracts with vendors responsible for network administration, driver's license and Motor Voter processes, administration of the SURE Help Desk, and the staff augmentation vendor.

- Reviewed news articles related to election threats such as the Russian involvement in the 2016 presidential election.

- Attended SURE training provided by DOS to gain an overview of how SURE works, what functionality SURE includes and how the counties use SURE to process applications, conduct list maintenance activities, and print poll books.

- Reviewed a list of SURE training DOS provided to counties, both prior to and during the audit period, to determine which counties requested and received training in addition to the initial training provided during the implementation of the SURE system.

- Judgmentally selected and visited seven county election offices between July 11, 2018 and September 11, 2018, to gain an understanding of how the counties process applications in SURE, including performing steps to review: the counties' procedures to detect duplicate registrations; the counties' procedures to conduct the HAVA check, and correspondence mailed to applicants requesting information required to complete the processing of applications. Two of the seven counties visited were at the recommendation

of DOS and the remaining five counties were selected in order to gain variety in geographic location and the number of voter registrations.

- Sent a survey (See copy in *Appendix H*) to all 67 counties in Pennsylvania (including the seven visited) to obtain similar information as gained during the visits such as processing information in SURE, equipment utilized, and security protocols. A total of 65 of the 67 counties provided responses to our questions either during the on-site visit interviews or by returning the survey; however, not all of the counties responded to every question in the survey.

- Included technical experts from the DAG's Bureau of Information Technology Audits as part of the audit team for data analysis and information systems assessment pertinent to our audit objectives.

- Consulted with a network administration expert from DAG's Office of Information Technology and Support Services for specialized network and cybersecurity knowledge.

- Consulted with cybersecurity audit experts from other state auditor offices on applicable cybersecurity control frameworks and auditor access to outside security assessments of critical infrastructure.

- Reviewed and analyzed redacted network and system diagrams of the SURE system in an attempt to obtain a thorough understanding of the various environments.

- Reviewed and analyzed redacted documents regarding the software, hardware, and operating systems supporting the SURE system.

- Reviewed and analyzed functional specifications documents for interfaces, where provided, and assessed the impact of interfaces between SURE and other systems.

- Reviewed DOS organizational charts with DOS officials to gain an understanding of the management structure.

- Reviewed the following reports from other organizations on voting system security and voter registration security to identify relevant security protocols and issues:

    - Brennan Center for Justice. *Defending Elections: Federal Funding Needs for State Election Security,* July 18, 2019.
    - Center for American Progress. *Election Security in All 50 States: Defending America's Elections*, February 12, 2018.

- U.S. Department of Justice. *Report on the Investigation into Russian Interference in the 2016 Presidential Election (also known as the Mueller Report)*, March 31, 2019.
- The Heritage Foundation. *A Sampling of Election Fraud Cases from Across the Country*. April 2017.
- State of Minnesota, Office of the Legislative Auditor. *Voter Registration: 2018 Evaluation Report*. March 8, 2018.
- United States Election Assistance Commission (EAC). *2014 Statutory Overview*, January 2015.
- Press Release of Select Committee on Intelligence, United States Senate, *Senate Intel Committee Releases Unclassified 1st Installment in Russia Report, Updated Recommendations on Election Security*. Richard Burr, Mark Warner, Susan Collins, Martin Heinrich, James Lankford. May 8, 2019.
- Report of the Select Committee on Intelligence, United States Senate, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 1: Russian Efforts against Election Infrastructure with Additional Views*. Released July 25, 2019.
- The University of Pittsburgh Institute for Cyber Law, Policy and Security. *The Blue Ribbon Commission on Pennsylvania's Election Security: Study and Recommendations*, January 4, 2019.
- The National Academies of Sciences, Engineering, and Medicine. *Securing the Vote: Protecting American Democracy*, September 6, 2018.
- Technology Science. *Voter Identity Theft: Submitting Changes to Voter Registrations Online to Disrupt Elections*, September 06, 2017.

- Received a signed affidavit from the Chief Information Security Officer (CISO) of the Employment, Banking, and Revenue (EBR) Delivery Center of the Office of Administration Office of Information Technology (OA/OIT) describing certain controls in place over the SURE system.

- Interviewed the CISO of the EBR Delivery Center for a verbal briefing on the contents of external security assessment reports issued by the United States Department of Homeland Security and reports issued by private firms contracted to assess security of the SURE system.

- Attended a presentation by the CISO of the Commonwealth providing an overview of OA/OIT's implementation of the National Institute of Standards and Technology Cybersecurity Framework.

- Received letters through DOS from two vendors summarizing security assessments performed on election systems.

- Reviewed working papers testing information technology general controls compiled in prior audits of the Commonwealth's Comprehensive Annual Financial Report.

- Reviewed a Service Organization Control (SOC) report for one vendor significant to the SURE system and attempted to review SOC reports for other relevant vendors.

- Reviewed the following policies governing internal controls, IT management, procurement, IT security, and cybersecurity issued by OA/OIT and DOS:

    - Commonwealth of Pennsylvania Information Technology Policy (ITP) ITP-SEC000 – *Information Security Policy*. May 2016.
    - ITP-SEC007 – *Minimum Standards for IDs, Passwords, and Multi-Factor Authentication*. March 1, 2006.
    - ITP-SEC015 – *Data Cleansing Policy*. May 1, 2013.
    - ITP-SEC019 – *Policy and Procedures for Protecting Commonwealth Electronic Data*. November 16, 2007.
    - ITP-SEC020 – *Encryption Standards for Data at Rest*. August 17, 2007.
    - ITP-SEC023 – *Information Technology Security Assessment and Testing Policy*, April 19, 2007.
    - ITP-SEC024 – *IT Security Incident Reporting Policy*. August 2, 2012
    - ITP-SEC025 – *Proper Use and Disclosure of Personally Identifiable Information*. March 19, 2010.
    - ITP-SEC031 – *Encryption Standards for Data in Transit*. August 17, 2007.
    - Commonwealth of Pennsylvania Information Technology Operations Document (OPD) OPD-SEC007A – *Configurations for IDs, Passwords, and Multi- Factor Authentication*. March 1, 2006.
    - Commonwealth of Pennsylvania Management Directive (MD) MD-205.34 – *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*. Amended January 22, 2016.
    - MD-325.12 – *Standards for Internal Control for Commonwealth Agencies*. Effective July 1, 2015.
    - MD-325.13 – *Service Organization Controls*. Effective November 22, 2017.
    - MD-535.9 – *Physical and Information Security Awareness Training*. October 3, 2006.
    - Commonwealth of Pennsylvania *Information Security Incident Response Procedures* (IRP) V2.11. November 11, 2008.
    - DOS Bureau of Election Security and Technology, Bureau of Elections and Notaries, Bureau of Campaign Finance and Civic Engagement. *Continuity of Operations Plan.* January 02, 2019.
    - DOS *Guidance on Electronic Voting System Preparation and Security*. September 2016.
    - DOS *Policy on Election System Security Measures*, Version 1.1, issued April 23, 2019.

- DOS *SURE Equipment Use Policy*. September 12, 2003, updated February 29, 2012.

- Reviewed the redacted results of the 2018 test of the SURE Emergency Recovery System conducted by DOS management.

- Inquired of DOS management about the applicability of Commonwealth IT policies to county election offices and IT personnel.

- Reviewed transcripts of the U.S. Senate Select Committee on Intelligence hearing on Election Security, March 21, 2018, the Pennsylvania House of Representatives State Government Committee hearing on Election Integrity and Reforms, October 15, 2018, and the U.S. House of Representatives Committee on Homeland Security hearing on Building Partnerships to Protect America's Elections, February 13, 2019.

- Reviewed the Center for Internet Security (CIS) *Critical Security Controls*, Version 7.1, the CIS *Handbook for Elections Infrastructure Security*, Version 1.0, dated February 2018, and the United States Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (DHS-CISA) publication entitled *Best Practices for Securing Election Systems*, issued May 21, 2019, to assist in developing our audit approach for testing cybersecurity controls.

- On February 25, 2019, the Auditor General traveled to Washington D.C. to meet with representatives of the Department of Homeland Security (Homeland Security) to discuss protocol regarding access to security reports issued by Homeland Security.

- Attempted to perform tests of design of information technology general controls in place over the SURE system in the following baseline control areas:
  - Access management
  - Change management (i.e., configuration management)
  - Segregation of duties
  - Service delivery
  - Business continuity/Disaster recovery.

- Reviewed the SURE database schema, data dictionary, and other database documentation to assist in documenting an understanding of the database and requesting data.

- Obtained from DOS electronic data files of all currently registered voters as of October 9, 2018 (referred to as the Voter Table) and the electronic history of all changes to voter records, such as changes to the voter's name and address that were recorded from January 1, 2016 through October 9, 2018 (referred to as the Application Table). We also obtained copies of each county's Pennsylvania Full Voter Export List as of October 9, 2018, from

the SURE system available to the public through the Department of State (DOS) website (referred to as the Full Voter Export Table).

- Obtained death data from the DOH of deaths recorded in Pennsylvania from October 2010 through October 2018 to compare to voter registration data as of October 9, 2018 to determine if any of the deceased remain as registered voters in SURE.

- Obtained the Social Security Administration's Death Master File of deaths as of August 2010 to determine if any of the deceased are still listed as registered voters in SURE.

- Using data analysis on the Voter Table we performed the following:

  - Tested for duplicate driver's license numbers as well as tests for other potential duplicate records based on first name, last name, date of birth (DOB), and/or last four digits of the Social Security number (SSN).

  - Searched for voters who were 100 years old or older as of October 9, 2019 and for voter registration dates that were prior to the voter's DOB. We then reviewed the U.S. Census Report entitled, *Centenarians:2010*, to compare against the numbers of voter records with dates of birth indicating the voter may be 100 years of age or older.

  - Compared the voter records to the DOH death data based on first name, last name, DOB, and/or the last four digits of the SSN.

  - Compared the voter records to the Social Security Death Master File data as of August 2010 based on first name, last name, DOB, last four digits of SSN, and street name. No additional potentially deceased voters were identified from this data matching procedure.

  - Reviewed voter records associated with potential duplicates or potential deceased voters to determine if votes were cast more than once per record or after the deceased date, as applicable. We did not believe our evidence was sufficient to report in a finding but did report our results to DOS to further investigate.

  - Determined the number of voter records remaining in active status despite having no activity for five or more years.

  - Determined the number of inactive voter records that should have been cancelled after failure to vote in the following two federal general elections.

- Using data analysis on the Application Table, we determined the following:

  - Whether list maintenance activities were being performed by each county and whether voter records were being cancelled for list maintenance activities within 90 days of the 2016 general election.

  - The number of pending applications and the length of time the applications remained in pending status.

- Using data analysis, we evaluated the design and operating effectiveness of application controls in place to prevent and/or detect: duplicate voter records, inaccurate dates of birth, inaccurate registration dates, potentially deceased voters, as well as controls to prevent inappropriate cancellation of voter records within 90 days of an election, controls to ensure residential addresses are within Pennsylvania, and controls to ensure the street name field does not include the street number.

- Judgmentally selected voter records and traced them to the SURE portal in order to investigate and analyze the following:

  - Information that appeared to be different among the Voter Table, the Full Voter Export Table, and the Application Table.

  - Pending records that appeared to have been replaced by a newer, approved voter application.

  - Records where it appeared that the DOB had been changed.

- Selected a random statistical sample, based on a confidence level of 98 percent and a tolerable error rate of two percent, of 196 voters from the total population of 8,567,700 voters registered in SURE as of October 9, 2018 with the intent of reviewing source documents to confirm the accuracy of the following information maintained in SURE for the 196 voters:

  - Full name (first, last, and middle name or initial, if included)
  - Address
  - DOB
  - Last four digits of the SSN (if included)
  - Last four digits of the Pennsylvania driver's license number or Pennsylvania identification number (if included)
  - Date registered
  - Party affiliation

We also planned to verify that each record had a signature image in the SURE system.

Source documents included applications or other documents provided by voters to update their voter record and were submitted by the voter either through a paper application, the Motor Voter process at Pennsylvania driver's license centers, or DOS' online application.

- Reviewed examples of emails sent from the Help Desk to DOS management regarding the progress of each county for specific tasks, such as list maintenance activities and poll book printing.

- Performed procedures to determine if list maintenance activities were performed by the counties such as the following:

  - Reviewed records in the Application and Voter Tables to determine if each county recorded list maintenance codes indicating that list maintenance activities had been performed.
  - Observed, during county visits, county staff processing documents from voters in response to list maintenance correspondence sent to them by the county.
  - Observed during testing of 196 voter's records that records had been updated as a result of information provided by voters in response to list maintenance procedures performed by the county.

- Reviewed a redacted November 2018 Election Support Plan that includes tasks that must be completed leading up to and after Election Day. Tasks include poll book printing by the counties, certification of voter registration numbers, and certification of the results following Election Day.

- Reviewed the Electronic Registration Information Center's (ERIC) website for information regarding when it was created, accomplishments since its inception, the member states, the cost of being a member, as well as what ERIC provides to its members.

- Reviewed examples of the letters sent by DOS to those identified by a tenured Associate Professor of Political Science hired by DOS as potential non-citizens that were not eligible to be registered voters. The letters included 7,702 dated April 27, 2018; 11,198 dated June 12, 2018; and 8,707 dated June 29, 2018.

- Reviewed documents from DOS regarding actions taken by DOS resulting from the responses received to the letters mailed to those identified as potential non-citizens.

- Reviewed screen shots of the Motor Voter process that was in place when non-citizens were permitted to register to vote.

- Reviewed screen shots of the Motor Voter process after the non-citizen issue was corrected by PennDOT, in conjunction with DOS.

- Visited a PennDOT Photo License Center to observe scenarios where a customer, with their camera card, came into the license center to obtain a new driver's license or renew their existing driver's license. The scenarios included:

    - Citizen either over 18 years of age or will be 18 by the date of the next election
    - Non-citizen of any age
    - Naturalized citizen over the age of 18

- Reviewed U.S. Election Assistance Commission, *Grant Expenditure Report Fiscal Year 2018*, dated April 4, 2019, to determine funding provided to states to financially help implement the requirements of HAVA.

- Reviewed the Commonwealth's SAP accounting system report, "Detail Grant Line Items by FM Posting Date" to determine expenditures made during fiscal years 2002 through 2013 from the federal funds received to improve the administration of federal elections.

Data Reliability

Government Auditing Standards requires us to assess the sufficiency and appropriateness of computer-processed information that we used to support our findings, conclusions, and/or recommendations. The assessment of the sufficiency and appropriateness of computer-processed information includes considerations regarding the completeness and accuracy of the data for the intended purposes.[130]

- To assess the completeness and accuracy of the data files from the SURE system of 1) all currently registered voters (the Voter Table), 2) the history of all of the changes made to voter records (the Application Table), and 3) the Pennsylvania Full Voter Export List, we conducted audit procedures as follows:

    - Obtained a management representation letter from DOS management confirming that the data provided to us had not been altered and was a complete and accurate duplication of the data from its original source.

[130] U.S. Government Accountability Office. *Government Auditing Standards*. 2011 Revision. Paragraph 6.66.

- Compared record counts to DOS' unaudited annual report of voter statistics, *The Administration of Voter Registration in Pennsylvania: Report to the General Assembly*, submitted by DOS for the calendar year ended December 31, 2017 sent to the General Assembly in June of 2018 to determine the completeness of the information provided. A variance of 1.3% was noted but determined to be reasonable given the timing differences between the report date and receipt of the data.

- Compared data among the three tables obtained from SURE to determine whether the data was accurate and if records were missing. Variances were investigated and ultimately we determined the data to be internally consistent.

- Using data analysis, compared total voter statistics per the data file of all currently registered voters as of October 9, 2018, to the unaudited annual report of voter statistics, *The Administration of Voter Registration in Pennsylvania: Report to the General Assembly*, submitted by DOS for the calendar year ended December 31, 2018, to test the voter data for completeness.

- Obtained reports from PennDOT's Motor Voter program and compared those records to application data within the SURE system to determine completeness.

- Obtained reports from DOS of initial voter application records submitted through PennDOT's Motor Voter system between January 1, 2016 and October 9, 2018, and compared them to the initial applications recorded as received from PennDOT in SURE. Although variances were noted, we found the count of applications sent and recorded to be substantially accurate.

- Attempted to evaluate the design and operating effectiveness of information technology general controls. DOS, however, refused to provide access to the contents of external security reports and other documents needed to perform the evaluation. See scope limitation above and in *Finding 1 (Scope Limitation A)*.

- Used obituaries to confirm a judgmental selection of potentially deceased individuals' first and last name, date of death, and city of residence. We also confirmed the DOB and middle initial if noted in the obituary. These additional tests were performed to validate the reliability of the match between DOH data and SURE data.

- Used Google Maps to confirm for a judgmental selection of records that the street address was within Pennsylvania in order to confirm the accuracy of the *State* field in the voter record and to provide additional evidence as to the eligibility of the voter.

- Randomly selected a sample of 196 records from the 8,567,700 registered voters in Pennsylvania and traced the information back to the source documentation maintained at the county election offices. We were unable to perform these audit procedures for 138 sampled items due to lack of cooperation from the counties, lack of cooperation from PADOT to provide information from the Motor Voter applications, lack of auditable information for online applications, and lack of sufficient record retention requirements and guidance. See the description of the scope limitation above and in *Finding 1 (Scope Limitation B)*.

Based on the procedures we were able to perform, as well as the procedures we were not able to perform due to scope limitations, in accordance with *Government Auditing Standards*, we concluded that the voter registration data extracted from the SURE system had significant limitations. However, due to the close approximation to independently produced reports issued by DOS and the consistency of the data among the three tables, we determined the data to be sufficiently reliable, with significant limitations, to support our findings and recommendations as noted throughout our report.

As noted in *Finding 4* in the report, we did not perform tests to validate the reliability of the "date last voted" field within the voter table. According to SURE job aids, the "date last voted" field is entered into SURE when poll workers scan the bar code (found beside the voter's signature in the poll book) after each election. While the process described appeared reasonable to capture voting dates, since we did not perform tests of the accuracy of the "date last voted" field, we determined this data field to be data of undetermined reliability. The data, however, was the best data available and although this determination may affect the precision of the numbers presented, as noted in *Finding 4*, there is sufficient evidence to support our findings and conclusions that DOS should work with the counties to investigate instances of potentially inactive voters who had not voted in the last two federal general elections and whose voter records may need to be cancelled.

- We did not perform procedures to assess the completeness and accuracy of the data of deceased individuals from the Pennsylvania Department of Health, the data from the Social Security Death Master file, and data from the US Census Bureau. We determined this data to be data of undetermined reliability, as noted in *Finding 2* of this report. This data was the best data available, however, and although this determination may affect the precision of the numbers presented of potentially deceased individuals and those over the age of 100, as noted in *Finding 2*, there is sufficient evidence to support our findings and conclusions.

- We did not perform procedures to assess the completeness and accuracy of the number of letters that DOS sent to voters identified as having questionable voter registration eligibility and the actions that subsequently occurred with each of the voters identified. We determined this data to be data of undetermined reliability, as noted in *Appendix D* of

this report. This data was the best data available, however, and although this determination may affect the precision of the number of individuals identified as potentially ineligible to vote, as noted in *Appendix D*, there is sufficient evidence to support the information noted in *Appendix D*.

Appendix B — Interagency Agreement Between the Department of State and the Department of the Auditor General

On May 15, 2018, the Department of the Auditor General (DAG) entered into an Interagency Agreement (agreement) with the Department of State (DOS) to perform an audit of DOS' Statewide Uniform Registry of Electors. The originally agreed upon date to provide DOS with the audit report was January 31, 2019. Due to delays by DOS in providing DAG requested audit information, the agreement was amended to:

- Extend the report release date to **July 31, 2019.**
- Further extend the report release date to **September 27, 2019**.
- Further extend again the report release date to **November 29, 2019.**

The following is a copy of the original agreement between DAG and DOS:

Doc. No. 2018-IA-002

INTERAGENCY AGREEMENT

This Interagency Agreement ("Agreement") is entered into by and between the Department of State ("DOS") and the Pennsylvania Department of the Auditor General ("Auditor General") for an audit of DOS' Statewide Uniform Registry of Electors ("SURE").

Sections 501 and 502 of *The Administrative Code of 1929* (71 P.S. §§181 and 182) require Commonwealth departments, boards, commissions, and agencies to coordinate their work and activities with other Commonwealth departments and agencies.

DOS, through its Bureau of Commissions, Elections and Legislation ("BCEL"), oversees the administration of the Commonwealth's electoral process which includes voter registration. To ensure a complete and accurate statewide voter registration system, DOS, pursuant to the dictates of the Help America Vote Act ("HAVA"), 52 U.S.C. § 21083(a), and the Pennsylvania voter registration law, 25 Pa.C.S. § 1201(3), administers the SURE system. Part of DOS' responsibility under the law involves maintenance of the database which ensures that the voter registration rolls are accurate and up to date. *Id.* § 21083(b).

The Auditor General is the chief fiscal watchdog of the Commonwealth. The Auditor General's mission is to serve the people of Pennsylvania by improving government accountability, transparency, and the effective use of taxpayer dollars. The Agency is responsible for using audits to gauge whether government programs and activities are meeting stated goals and objectives and to ensure that all state money is spent legally and properly.

DOS has requested that the Auditor General perform an audit of the SURE system to assess its accuracy, operability, and efficiency and DOS has agreed to provide access to the SURE system for the purposes of this audit to the Auditor General under the terms and conditions of this Agreement.

The parties, intending to be legally bound, agree as follows:

1. DOS Responsibilities. DOS shall:
   a. cooperate with the Auditor General's requests involving the proposed audit;
   b. to the extent feasible, provide the Auditor General with read-only, point in time access to the SURE system data for the purpose of conducting the proposed audit;
   c. provide training and ongoing technical assistance to the Auditor General regarding DOS methods of accessing and updating records in the SURE system.

d. pay the Auditor General up to One Hundred Thousand Dollars ($100,000.00) for the expenses associated with conducting the proposed audit. Monthly invoices shall be submitted by the Auditor General to DOS by the 15th day of the following month.

2. Auditor General Responsibilities.

a. The Auditor General shall conduct an audit of the SURE system and provide a report to DOS no later than January 31, 2019. The report shall include all of the following:

i. Assessment of whether records maintained within the SURE system are accurate and in accordance with the Help America Vote Act (HAVA) and Pennsylvania law;

ii. Evaluation of the process for input and maintenance of voter registration records;

iii. Review of security protocols of the SURE system;

iv. Review of the efficiency and accuracy of the SURE system;

v. Review of the internal controls, methodology for internal audits and internal audits review process;

vi. Review of the external controls, methodology for external audits and external audits review process;

vii. Review of the methodology for the issuance of directives and guidance to the counties by DOS regarding voter registration and list maintenance; and

viii. Any other relevant information or recommendations related to the accuracy, operability, and efficiency of the SURE system, as determined by the Auditor General.

b. Audit progression: To the extent feasible, the Auditor General will meet and confer with DOS to provide DOS quarterly audit updates.

c. Audit period: The audit period will be January 1, 2016, through the end of the audit procedures. This will include auditing the processes that were in place for that time period. This will also include testing the accuracy of the data as of a

point-in-time that has not been determined, but preferred to be as current as possible. The Auditor General will ensure that the data accuracy is tested from several sources covering different time periods that will be finalized during the audit.

d. Report information: The information contained with the report shall not include data, documentation, configuration representations, product or supplier names, network addresses, or other critical information that may interfere or jeopardize the security, privacy, or integrity of the SURE system or any of the Commonwealth's or counties' networks or systems. The Auditor General shall coordinate and work in conjunction with DOS to determine what is to be treated as restricted content prior to issuance of the final report.

3. Data Security.

a. The Auditor General and DOS will comply with all federal and state laws and regulations pertaining to any data exchanged pursuant to this Agreement.

b. The Auditor General and DOS will ensure that all data exchanged pursuant to this Agreement is secure, privacy is protected and integrity is maintained as required by OA/OIT requirements.

c. The Auditor General will destroy all data that has been provided by DOS once the data is no longer needed.

d. Only authorized personnel in the Auditor General's Office and DOS with a business need will have access to the data exchanged pursuant to this Agreement.

4. General Provisions.

a. Term. This Agreement will become effective as of the Effective Date, as defined below, and will remain in effect until the final audit report is delivered and accepted by the parties on or before January 31, 2019, unless earlier terminated by either party in accordance with Paragraph 4(c) of this Agreement.

b. Effective Date. The Effective Date of this Agreement shall be May 15, 2018, prior to which the Agreement shall be fully executed by both parties and all approvals required by Commonwealth contracting procedures obtained.

c. Termination. Either party may terminate this Agreement for good cause by sending thirty (30) days prior written notice of termination to the other party

d. Amendments and Modifications. No alterations or variations to this Agreement shall be valid unless made in writing and signed by the parties. Amendments to this Agreement shall be accomplished through a formal written document signed by the parties with the same formality as the original Agreement.

e. Full Understanding of the Parties. This Agreement sets forth the full and complete understanding of the Parties.

f. Agency. The employees or agents of each party who are engaged in the performance of this Agreement shall be employees or agents of that party and shall not be considered for any purpose to be employees or agents of the other party.

g. Notice. Any written notice to DOS under this Agreement shall be sufficient if mailed to:

Chief Counsel
Pennsylvania Department of State
401 North Street
Room 306, North Office Building
Harrisburg, PA 17120

Any written notice to the Agency under this Agreement shall be sufficient if mailed to:

Chief Counsel
Department of the Auditor General Finance Building
613 North Street, Room 224
Harrisburg, PA 17120-0018

h. Applicable Law. This Agreement shall be governed by, and interpreted and enforced in accordance with, the laws of the Commonwealth of Pennsylvania and the decisions of the Pennsylvania courts.

i. Disputes. Any dispute arising hereunder shall be submitted to Office of General Counsel for final resolution.

j. Severability. The provisions of this Agreement shall be severable. If any phrase, clause, sentence or provision of this Agreement is declared to be contrary to the Constitution of Pennsylvania or of the United States or of the laws of the Commonwealth, the applicability thereof to any government, agency, person or circumstance is held invalid, the validity of the remainder of this Agreement and the applicability thereof to any government, agency, person or circumstance shall not be affected.

k. Integration. When fully executed by the parties, this Agreement shall be the final and complete Agreement between the parties containing all the terms and conditions agreed on by the parties. All representations, understandings, promises and agreements pertaining to the subject matter of this Agreement made prior to or at the time this Agreement is executed are superseded by this Agreement, unless specifically accepted by any other term or provision of this Agreement. There are no conditions precedent to the performance of this Agreement, except as expressly set forth in this Agreement.

[SIGNATURE PAGE FOLLOWS.]

The parties, through their authorized representatives, have signed this Agreement below.

Robert Torres 5/15/18
Robert Torres — Date
Acting Secretary
Department of State

Eugene A. DePasquale 5/14/18
Eugene A. DePasquale — Date
Auditor General

APPROVALS AS TO FORM AND LEGALITY:

5/15/18
Office of Chief Counsel — Date
Department of State

5-14-18
Office of Chief Counsel — Date
Pennsylvania Department of the
Auditor General

Pamela J. Cross 5/16/18
Office of General Counsel — Date

5/21/18
Office of Attorney General — Date

John Ondaff 5/31/2018
Comptroller Operations — Date

RECEIVED
2018 MAY 21 PM 3:10
BUREAU OF
FINANCE & OPERATIONS

Appendix C | Voter Registration Process

The voter registration process in Pennsylvania is conducted by county election offices (counties) but involves a partnership with the Department of State (DOS). The National Voter Registration Act and Pennsylvania law requires that the Pennsylvania Department of Transportation (PennDOT) provide a voter registration opportunity to its customers. This process is commonly referred to as Motor Voter.[131] The Motor Voter process provides PennDOT customers the opportunity to register to vote, or change their address if they are currently registered to vote, while receiving or renewing their driver's license (DL) or photo identification (ID) card at a PennDOT photo license center, as well as the ability to update their registration in-person and online.

In addition, applicants have the option to register to vote via paper application, online, and for any person that utilizes the services of various government assistance offices, the person is asked if they want to register at the time of application for benefits or re-certification for benefits.[132] A paper application can be obtained online or at the county and returned to the county by mail or in-person once completed. Online applications are managed by DOS and can be accessed by visiting register.votesPA.com.

Regardless of which application method one chooses, the information required to register is the same. The applicant must provide information including their full name, date of birth, residence address, mailing address (if different than residence), and political affiliation. Applicants are also prompted to provide their DL or ID number and/or the last four digits of their Social Security number (SSN) in order to help verify the applicant's identity; however, the county cannot deny an application if the applicant does not provide their DL or ID number or SSN.[133] The applicant must also confirm that they are eligible to register to vote by answering eligibility questions included on the application and signing the application.

Federal and State law establishes eligibility requirements for residents to register to vote.[134] Eligibility criteria include a minimum age requirement of 18 years of age and citizenship of the

[131] 52 U.S.C. § 20504. *See also* 25 Pa.C.S. § 1323.
[132] 25 Pa.C.S. § 1325. Consistent with the NVRA, the offices in Pennsylvania that have been identified as those that "provide public assistance" for voter registration purposes are: Women, Infant and Children Nutrition Clinics; County Assistance Office; Clerk of Orphans' Courts; Children and Youth Agencies; Area Agencies on Aging; Para-Transit providers; Special Education Programs at the 14 state-owned universities; agencies serving people with disabilities and County Mental Health/Intellectual Disabilities offices; and the armed services recruitment centers. *The Administration of Voter Registration in Pennsylvania, 2017 Report to the General Assembly, June 2018*, page 10.
[133] 25 Pa.C.S. § 1328. The Pennsylvania Voter Registration Application includes a box for the applicant to check if they do not have a PA driver's license or a PennDOT identification card or a Social Security number. All first time voters must show identification at the polling place. The approved list of identification documents can be found at http://www.votespa.com.
[134] 52 U.S.C. § 10701 (Enforcement of the 26th Amendment). Note that HAVA has statutory provisions prohibiting certain discriminatory voting acts, such as poll taxes, in Chapter 103. *See also* 25 Pa.C.S. § 1301(a).

United States (U.S.), the Commonwealth of Pennsylvania, and the applicable district. It should be noted, however, that neither state nor federal law require proof of citizenship in order to register to vote, regardless of the method of application. Neither DOS nor the counties conduct a review to confirm the citizenship of an applicant. When an applicant completes a voter registration application, whether on paper, online, through a voter registration drive, or similar method, they are merely asked to sign a declaration (without providing any validation), which states the following:

- I am a United States citizen and will have been a citizen for at least one month on the day of the next election.
- I will be at least 18 years old on the day of the next election.
- I will have lived at the same address in Section 5 [of the application] for at least 30 days before the election.
- I am legally qualified to vote.[135]

The applicant must indicate by checking a box that: "I affirm that this information is true. I understand that this declaration is the same as an affidavit, and, if this information is not true, I can be convicted of perjury, and fined up to $15,000, jailed for up to 7 years, or both."[136] Given that the law ***does not*** require proof that the applicant's declaration/affirmation is valid, it is possible that an ineligible person, including a non-citizen, could apply to register to vote regardless of whether they knew they were violating the law or if it was done unintentionally, as with those that may not fully understand the questions being asked and statements made due to a language barrier.[137] Regardless of the circumstances, as previously reported, there is a potentially substantial criminal penalty for those found to have provided false information.

Requiring applicants to submit proof of citizenship has been attempted in other states and has been met with court challenges. In June 2018, in a matter involving private citizens represented by several public interest organizations on behalf of the League of Women Voters of Kansas against the Kansas Secretary of State, a federal district court judge found that Kansas could not require documentary proof of U.S. citizenship when registering to vote, because such laws

[135] This declaration is provided in Section 11 of the application.
[136] Ibid.; the application also contains the following notice: "PENALTY FOR FALSIFYING DECLARATION WARNING: If a person signs an official registration application knowing a statement declared in the application to be false, makes a false registration, or furnishes false information, the person commits perjury. Perjury is punishable, upon conviction, by a term of imprisonment not exceeding seven years, or a fine not exceeding $15,000, or both, at the discretion of the court. Submitting an application containing false information may also subject a person to other penalties, including loss of the right of suffrage, under state or federal law." This is commonly referred to as "signing under penalty of perjury" and is enforceable under 18 Pa.C.S. § 4902.
[137] At a 2016 hearing, a former DOS election official claimed that a "glitch in the state's driver licensing software 'may inadvertently register' noncitizen immigrants to vote without their knowledge." <https://thehill.com/blogs/blog-briefing-room/news/357143-pa-officials-find-hundreds-of-illegal-ballots-cast-in-state> (accessed April 29, 2019).

violate the constitutional right to vote.[138] The decision, which is currently under appeal, invalidated Kansas' proof-of-citizenship registration law.[139] In the meantime, however, the holding of the case has national implications, including in Pennsylvania.

To date, the Pennsylvania General Assembly has not attempted to require proof of citizenship to register to vote, but did attempt to enact a voter identification (Voter ID) law in 2012.[140] Pennsylvania's Voter ID law would have required all voters to show specific photo identification at the polling place before being allowed to cast their ballot. The Voter ID law specified that the photo identification must include an expiration date, therefore invalidating several forms of photo identification, including many employee identification cards. Before the law could take effect, however, a lawsuit was filed in Pennsylvania's Commonwealth Court, alleging that the new Voter ID law violated Pennsylvania's Constitution by depriving citizens of their most fundamental constitutional right — the right to vote. The lawsuit sought an injunction blocking enforcement of the law before the November 2012 election.[141] Ultimately, the law was struck down by the Pennsylvania Commonwealth Court, before voters were subject to the new requirements in the next election, and Pennsylvania returned to its original first-time voter identification requirement.[142]

The ability to register to vote ends 30 days prior to any election.[143] Therefore, a person wishing to register for the first time, change their name, address, or party affiliation must submit a completed voter registration application no later than 30 days prior to the next election. Any paper application postmarked after the cut-off is to be processed after the election is finalized. If the applicant applies online, they have until 11:59 P.M. and 59 seconds on the day of the cut-

---

[138] *Fish v. Kobach*, 309 F. Supp. 3d 1048 (D. Kan. 2018). The matter has been appealed to the United States Court of Appeals Tenth Circuit. On January 14, 2019, the party name of the defendant Kris Kobach has been updated to reflect a change in the state of Kansas' Secretary of State to Scott Schwab as follows: *Fish v. Schwab*. See <https://www.courtlistener.com/docket/4510003/fish-v-kobach/?filed_after=&filed_before=&entry_gte=&entry_lte=&order_by=desc> (accessed April 29, 2019).
[139] Ibid.
[140] Former Act 18 of 2012 was held unconstitutional by the Pennsylvania Commonwealth Court and its enforcement permanently enjoined by *Applewhite v. Com.*, 2014 WL 184988 (Pa. Cmwlth. 2014).
[141] The lawsuit was filed by the American Civil Liberties Union of Pennsylvania, the Advancement Project, the Public Interest Law Center of Philadelphia, and the Washington, DC law firm of Arnold & Porter LLC, on behalf of ten Pennsylvania voters and three prominent advocacy organizations. <https://www.aclupa.org/news/2012/05/01/groups-file-lawsuit-in-commonwealth-court-to-overturn-pennsylvanias-unconstitutional-voter-photo-id-law> (accessed March 21, 2019).
[142] A first time voter, or a voter voting at a new polling place, must show proof of identification. The valid photo identifications include a Pennsylvania DL or PennDOT ID card, ID issued by any Commonwealth agency, ID issued by the U.S. Government, U.S. Passport, U.S. Armed Forces ID, student ID, or an employee ID. If you do not have a photo ID, a first time voter can use one of the following non-photo IDs that includes their name and address: confirmation issued by the County Voter Registration Office, non-photo ID issued by the Commonwealth, non-photo ID issued by the U.S. Government, firearm permit, current utility bill, current bank statement, current paycheck, or a government check. See <https://www.votespa.com/Register-to-Vote/Pages/Voter-ID-for-First-Time-Voters.aspx> (accessed March 20, 2019).
[143] 25 Pa. C.S. § 1326(b).

off.[144] Through Motor Voter at PennDOT, they have until the close of business of the photo license center on the day of the cut-off.

Once registered, a voter will remain registered until they either (1) request their voter registration be cancelled or (2) the county cancels the registration as part of its required list maintenance process.[145] A registered voter can cancel their voter registration at any time by completing and signing a "Request To Cancel Voter Registration" form and forwarding it to the county voter registration office in the county in which they are registered. A county may cancel a voter's registration in the process of performing the annual list maintenance that is required by law. List maintenance activities include cancelling a voter's registration due to death, moving out of the county or state, and not voting and not having any contact with the county elections office for a specified amount of time.[146] List maintenance is discussed in detail in *Finding 4*.

[144] DOS Election Support Plan "Verification and Environment changes."
[145] 52 U.S.C. § 21083(a)(2) (Computerized list maintenance). *See also* 25 Pa.C.S. §1901 (Removal of electors). A voter's county and/or voting precinct may change due to a change in residence within Pennsylvania, but the voter will still remain as a registered voter.
[146] 25 Pa C.S. § 1501.

Appendix D	The lack of oversight that allowed non-citizens the ability to register to vote at PennDOT's photo license centers, even after indicating they are not a citizen, was addressed during the audit period.

In 2017, media reports identified an issue in which non-citizens had the ability to register to vote at the Pennsylvania Department of Transportation (PennDOT) photo license centers.[147] We asked Department of State (DOS) management about this issue, and its responses are summarized below. We did not, however, have access to individuals' records of citizenship status and did not determine whether non-citizens were registered to vote.

According to DOS management, in 2017, DOS became aware of and took subsequent steps to investigate and address a decades-old issue with the Motor Voter process that allowed non-citizens the ability to register to vote even if they indicated that they are not citizens.[148] The issue, as explained by DOS management, was that when a person was offered the opportunity to register to vote during the driver's license (DL) photo card renewal/application process at PennDOT photo licensing centers, those that indicated that they were non-citizens *were not* excluded from the voter registration questions.[149] While voter registration during the DL photo card process requires an individual to twice confirm their citizenship status, both those that indicated they were citizens and those that indicated they were non-citizens were given the opportunity to register to vote.[150]

The National Voter Registration Act of 1993 (Motor Voter), which became effective on January 1, 1995, created requirements that each States' motor vehicle authority must: (1) provide individuals with the opportunity to register to vote at the same time that they apply for a DL or seek to renew a DL; and (2) forward the completed application to the appropriate state or local election official. In Pennsylvania, this was a manual process for many years due to each of the 67 counties having a different voter registration system. PennDOT mailed hard copy voter

[147] <https://philadelphia.cbslocal.com/2017/09/20/it-undermines-integrity-of-elections-glitch-allows-non-citizens-in-pa-to-vote/> (accessed May 17, 2019) and <http://www.mcall.com/news/pennsylvania/mc-nws-pa-voter-registration-glitch-non-citizens-20170920-story.html> (accessed May 17, 2019).

[148] On February 26, 2018, the Public Interest Legal Fund filed a complaint in the U.S. District Court for the Middle District of Pennsylvania seeking injunctive relief to compel DOS to allow the group access to information on non-citizen voting records. As of the date of this audit, the lawsuit is ongoing. See *PILF v. Torres*, 1:18-cv-00463 and 1:19-cv-00622. <https://freebeacon.com/issues/pennsylvania-state-dept-sued-hiding-noncitizen-voting-records/> (accessed July 26, 2019).

[149] Citizenship is determined based upon documentation that PennDOT requires individuals to provide, such as a birth certificate, U.S. Passport, or a Certificate of Naturalization.

[150] A person applying to register to vote is required to affirm that they are: (1) A citizen of the United States; (2) A resident of Pennsylvania and the election district in which they want to register for at least 30 days prior to the next election; and (3) At least 18 years of age on or before the next election.

registration applications to DOS which were subsequently forwarded to the appropriate county election office (county) for processing.[151] Once new federal and subsequent state laws were enacted and in effect, DOS implemented the Statewide Uniform Registry of Electors (SURE) system. With the creation of SURE, PennDOT's Motor Voter process was electronically connected to the SURE system.[152] When the last county implemented SURE in 2005, the Motor Voter process became fully automated, with applications from PennDOT being electronically received by SURE and then electronically parsed out to the respective counties for processing.

After the non-citizen voter registration issue related to Motor Voter was identified, PennDOT, in conjunction with DOS, made changes to the Motor Voter process to help ensure that those who indicate that they are non-citizens are no longer able to register to vote through PennDOT. DOS management stated that the project to correct the issue was completed in December 2017. We confirmed management's statement through observation of the Motor Voter process during a visit to a photo license center in November 2018. Currently, when a customer arrives at a PennDOT photo license center with their camera card to obtain a new DL or renew their existing DL, their citizenship status is embedded into the bar code on the camera card. Based on this bar code, a non-citizen customer is not asked the voter registration questions. Conversely, when a citizen (either over the age of 18 or who will be 18 by the date of the next election) arrives at a photo license center, they are asked the voter registration questions. We confirmed this process is in place by observing multiple scenarios at a PennDOT photo license center of individuals who were identified in the PennDOT system as non-citizens and citizens (both under age 18 and over age 18).

In addition to working with PennDOT to correct the issue, DOS management stated that steps were taken to investigate and address the concern that non-citizens were registered to vote. DOS management stated that they retained an expert, a tenured Associate Professor of Political Science, to conduct an analysis by comparing the Commonwealth's voter registration data with other available Commonwealth databases. We requested information from DOS regarding what Commonwealth databases were used for the analysis and the results of the analysis; however, DOS would not provide this information. Therefore, we were unable to verify the following:

- Whether DOS actually retained an individual to conduct an analysis.
- The scope and methodology of the analysis.
- The results and conclusions of the analysis.

[151] National Voter Registration Act of 1993 (Motor Voter), 52 U.S.C. §§ 20501–20511 (formerly 42 U.S.C. §§ 1973gg–1973gg-10).
[152] In 2002, the U.S. Congress passed the Help America Vote Act (HAVA) and, subsequently, the Pennsylvania General Assembly enacted Act 3 of 2002, which implemented HAVA into Pennsylvania Law. *See* 52 U.S.C. §§ **20901**-21145 (formerly 42 U.S.C. §§ 15301-15545) and **25 Pa.C.S.** §§ 1101-1906 (as noted in an earlier footnote, Act 3 of 2002 was added Part IV to the consolidated Title 25 Elections).

According to DOS management, a series of letters, of which examples of each were provided to us for review, were sent to the individuals identified as having questionable eligibility.[153]

April 27, 2018

7,702 letters mailed to **active** voters whose eligibility needed further confirmation.

June 12, 2018

11,198 letters mailed to **active and inactive** voters whose eligibility needed further confirmation. This included many from the 7,702 sent in the spring.

June 29, 2018

8,707 letters mailed to those that did not respond to the June 12th letter.

Following the series of letters shown above, DOS management stated that they placed robocalls to the identified individuals that had not responded to the letters from DOS.[154] As a result of these letters and robocalls, DOS management stated that the following actions occurred:

[153] The letters outlined the basic requirements to be a registered voter (as described above), and asked the recipient of the letter to affirm that they were qualified to be a registered voter or request that their registration be cancelled. Information regarding the number of letters sent by DOS was provided to us by DOS management. DOS management, however, did not provide any additional documentation to support the number of letters that DOS reportedly mailed to voters. DOS management indicated that most of the recipients of the April 27, 2018, letter also received the June 12, 2018, letter. If the individual had responded to DOS, however, then they would not have been sent the June 12, 2018, letter.

[154] A **robocall** is a phone call that uses a computerized autodialer to deliver a pre-recorded message. Robocalls were only made to those individuals that had a telephone number available in their voter record.

Actions that occurred with the 11,198 active and inactive voters whose eligibility needed further confirmation based on analysis performed – as represented by DOS management	
215	Requested that their voter registration be cancelled. No reason for cancellation was required to be given by the voter.[a/]
1,948	Affirmed that they were qualified to be a registered voter.
51	Failed to fully complete either the affirmation or cancellation form. Follow-up is being conducted by either DOS or the respective county election office.
286	Voter records were cancelled as a result of unrelated, routine list maintenance conducted by county election offices after the letters were mailed.
8,698	Voter names were forwarded to their respective county election office for further research to be performed to determine their eligibility.
11,198	**Total number of letters mailed to active and inactive voters whose eligibility needed further confirmation.**

[a/] - A request to cancel their voter registration by the recipient of the letter does not necessarily mean that the person is ineligible to be a registered voter. A person may decide that they no longer wish to be a registered voter for reasons other than ineligibility.

Source: This table was compiled by staff of the Department of the Auditor General based on information provided by DOS management. The data are of undetermined reliability as noted in Appendix A. However, this is the best data available. Although this determination may affect the precision of the numbers we present, there is sufficient evidence in total to support our conclusions.

DOS management stated that regarding the 8,698 names forwarded to the counties for follow-up, they have not conducted any follow-up with the counties, noting that it is the counties' obligation to take action to determine eligibility and/or remove ineligible voters as appropriate.

As a result of the decades-old issue with the PennDOT Motor Voter system, individuals who were ineligible to register to vote were in fact allowed to register and, therefore, may have voted in elections. Although the issue with the Motor Voter system has been corrected, DOS and counties must continue to address the concern that ineligible individuals may still be registered to vote.

Appendix E Voter Registration by County

Commonwealth of Pennsylvania Department of State Division of Voter Registration 2018 Voter Registration Statistics - Official November 6, 2018						
County	**Democratic**	**Republican**	**Green**	**Libertarian**	**Other Parties**	**All Parties**
Adams	19,557	36,652	92	449	10,275	67,025
Allegheny	546,641	261,938	1,259	4,964	126,226	941,028
Armstrong	14,419	22,211	34	243	4,443	41,350
Beaver	55,569	41,149	86	575	13,302	110,681
Bedford	7,906	20,587	21	128	2,845	31,487
Berks	116,018	100,459	436	1,613	38,091	256,617
Blair	22,453	44,132	82	382	8,948	75,997
Bradford	9,729	21,971	53	218	4,465	36,436
Bucks	196,280	185,919	647	2,893	71,496	457,235
Butler	40,697	69,840	117	785	17,018	128,457
Cambria	41,300	33,461	81	324	8,172	83,338
Cameron	1,029	1,526	4	13	346	2,918
Carbon	18,008	18,608	63	251	6,249	43,179
Centre	46,205	43,822	184	739	20,182	111,132
Chester	141,384	152,684	502	2,023	60,714	357,307
Clarion	7,354	12,909	21	93	2,533	22,910
Clearfield	17,051	24,359	42	235	5,202	46,889
Clinton	8,090	10,051	28	104	2,584	20,857
Columbia	14,500	18,187	42	256	5,695	38,680
Crawford	18,498	27,626	55	269	6,099	52,547
Cumberland	57,935	86,488	288	1,175	26,370	172,256
Dauphin	84,062	74,276	274	1,013	26,228	185,853
Delaware	188,908	162,271	432	1,498	50,262	403,371
Elk	8,578	8,588	23	77	2,080	19,346
Erie	96,961	68,402	321	1,041	25,185	191,910
Fayette	43,431	27,491	70	315	6,901	78,208
Forest	1,220	1,765	2	12	329	3,328
Franklin	24,150	54,942	89	512	12,898	92,591
Fulton	2,307	5,859	8	49	877	9,100
Greene	11,337	8,411	47	70	1,981	21,846
Huntingdon	9,033	17,749	50	105	3,078	30,015
Indiana	19,070	24,005	57	230	6,056	49,418

Jefferson	9,008	17,354	29	152	3,263	29,806
Juniata	3,718	8,642	16	50	1,373	13,799
Lackawanna	86,740	42,383	223	562	13,702	143,610
Lancaster	106,685	169,621	494	2,050	50,642	329,492
Lawrence	25,341	23,316	32	263	5,807	54,759
Lebanon	26,303	46,814	106	496	12,012	85,731
Lehigh	113,101	79,383	322	1,353	38,721	232,880
Luzerne	106,257	76,235	360	1,007	23,654	207,513
Lycoming	21,179	38,006	69	329	8,771	68,354
McKean	6,710	13,791	32	154	3,165	23,852
Mercer	30,385	31,721	67	349	8,955	71,477
Mifflin	6,805	15,248	20	130	2,502	24,705
Monroe	50,688	36,143	155	653	20,543	108,182
Montgomery	273,860	206,635	743	3,122	85,359	569,719
Montour	4,683	6,383	19	79	2,062	13,226
Northampton	96,393	73,561	322	1,335	37,702	209,313
Northumberland	19,249	26,646	82	290	6,518	52,785
Perry	6,814	18,079	28	188	3,384	28,493
Philadelphia	818,082	118,692	1,531	3,206	122,618	1,064,129
Pike	14,540	18,759	72	300	8,725	42,396
Potter	2,559	7,031	14	61	1,049	10,714
Schuylkill	31,749	43,763	114	448	9,845	85,919
Snyder	5,247	13,506	22	164	2,554	21,493
Somerset	15,546	26,903	30	190	4,330	46,999
Sullivan	1,467	2,449	6	21	433	4,376
Susquehanna	7,488	14,879	54	135	3,213	25,769
Tioga	6,902	16,228	42	153	3,434	26,759
Union	7,297	12,679	33	111	3,923	24,043
Venango	10,229	17,242	43	216	3,704	31,434
Warren	10,107	15,369	50	150	4,514	30,190
Washington	66,867	57,918	115	729	15,778	141,407
Wayne	9,772	18,171	71	194	5,131	33,339
Westmoreland	110,356	107,339	195	1,295	28,165	247,350
Wyoming	5,244	9,714	33	79	1,870	16,940
York	104,274	151,941	480	2,180	46,740	305,615
Totals	**4,111,325**	**3,270,882**	**11,534**	**44,848**	**1,171,291**	**8,609,880**

Source:<*https://www.dos.pa.gov/VotingElections/OtherServicesEvents/VotingElectionStatistics/Pages/Voter-Registration-Statistics-Archives.aspx*> (accessed June 21, 2019).

Note: The totals in the "2018 Voter Registration Statistics – Official" table above do not match the voter registration totals in the Voter Table data we received from the Department of State (DOS) due to a timing difference. The table above contains totals as of November 6, 2018, whereas, the Voter Table data we received from DOS was extracted

on October 9, 2018, and contains a total of 8,567,700 registered voters. As of June 17, 2019, the voter registration total as reported by DOS was 8,505,621. These changes in the number of registered voters are normal, since voter registration totals change daily due to the ongoing addition and maintenance of records.

Appendix F HAVA Funds Received by Pennsylvania

The United States Election Assistance Commission (EAC) and the United States General Services Administration (GSA), acting on EAC's behalf, awarded three non-discretionary grants, based on a predetermined formula, to states to financially help implement the requirements of the Help American Vote Act of 2002 (HAVA).[155] The following sections briefly explain these grants and show the breakdown of the $160.5 million of HAVA funds received and the amounts expended by Pennsylvania as of September 30, 2018.

Section 101: Payments to States for Activities to Improve Administration of Elections

Section 101 funds were provided to states for activities to improve the administration of federal elections and could be used for various purposes, such as voter education, development of the state plan, and training. GSA distributed a total of $349 million in Section 101 funds to states between April 2003 and August 2003.[156] These funds were required to be deposited in interest-bearing state election accounts and had no restrictions on when they could be expended by the states once obligated at the federal level. Pennsylvania received $11,323,168 in Section 101 funds and expended the funds and interest earned through state fiscal year ended June 30, 2013, as shown in the following table:

[155] EAC also administered three discretionary grant programs (Election Data Collection, College Poll Workers, and Mock Elections) that were awarded through a competitive process, and the United States Department of Health and Human Services administered a grant program to increase the accessibility of polling locations to disabled persons. These other grants were not included in this summary. Source: U.S. Election Assistance Commission, *Strengthening the Electoral System One Grant at a Time: A Retrospective of Grants Awarded by EAC April 2003 – December 2010,* <https://www.eac.gov/assets/1/6/FY2010_Grants_Report_FINAL.pdf> (accessed July 12, 2019).
[156] Ibid.

State Fiscal Year	Grant Expenditures	Interest Expenditures	Total Expenditures
2002	$ 115,738	-	$ 115,738
2003	$ 6,708,787	-	$ 6,708,787
2004	$ (345,881)	-	$ (345,881)
2005	$ 2,119,419	-	$ 2,119,419
2006	$ 1,644,302	-	$ 1,644,302
2007	$ 493,544	-	$ 493,544
2008	$ 540,638	-	$ 540,638
2009	$ 433,052	-	$ 433,052
2010	$ 142,912	$ 235,476	$ 378,388
2011	$ (711,851)	$ 817,782	$ 105,931
2012	$ 182,498	$ 156,541	$ 339,039
2013	$ 10	$ 91,693	$ 91,703
Total	**$11,323,168**	**$ 1,301,492**	**$12,624,660**

Source: Produced by the Department of the Auditor General staff from the Commonwealth's SAP accounting system report, "Detail Grant Line Items by FM Posting Date."

Section 102: Payments to States for Election Administration Improvements and Replacement of Punch Card and Lever Voting Machines

Section 102 funds were required to be used to replace any punch card or lever voting systems. GSA distributed a total of $300 million in Section 102 funds to states in federal fiscal year (FFY) 2003.[157] The deadline for states to have replaced its machines was originally November 2, 2004, however, states could file for subsequent extensions which ultimately expired on the date of the first federal election held after November 1, 2010.[158] States with unobligated funds after the deadline were required by HAVA to return the balance of funds to EAC for redistribution to all states in the form of Section 251 payments. Pennsylvania received $22,897,794 in Section 102 funds and expended the funds and interest earned through state fiscal year ended June 30, 2011, as shown in the following table:

[157] The federal fiscal year is October 1 through September 30.
[158] Ibid.

State Fiscal Year	Grant Expenditures	Interest Expenditures	Total Expenditures
2005	$ 10,658,762	-	$ 10,658,762
2006	$ 9,475,847	-	$ 9,475,847
2007	$ 1,370,102	-	$ 1,370,102
2008	$ 933,803	-	$ 933,803
2009	$ 2,551,075	-	$ 2,551,075
2010	$(2,169,751)	$ 4,002,558	$ 1,832,807
2011	$ 77,956	$ 261,616	$ 339,572
Total	**$ 22,897,794**	**$ 4,264,174**	**$ 27,161,968**

Source: Produced by the Department of the Auditor General staff from the Commonwealth's SAP accounting system report, "Detail Grant Line Items by FM Posting Date."

Section 251: Requirements Payments

Section 251 funds were required to be used to procure voting systems that comply with the new standards of HAVA, develop and implement a computerized statewide voter registration list, and other specific improvements. EAC disbursed a total of $2.6 billion in requirements payments in FFY 2003, 2004, 2008, 2009, 2010, and 2011. Section 251 funds and interest earned on deposits of Section 251 funds had no fiscal year limitation at the state level once obligated at the federal level.[159] Pennsylvania received a total of $112,821,809 in Section 251 funds. The following table shows the amount of funds received by Pennsylvania by FFY. As of September 30, 2018, Pennsylvania earned $16.8 million in interest and had total expenditures of $126.7 million, leaving a balance of $2.9 million in unspent funds.[160]

[159] Ibid.
[160] The U.S. Election Assistance Commission, *Grant Expenditure Report Fiscal Year 2018*, dated April 4, 2019, <https://www.eac.gov/assets/1/6/FY2018HAVAGrantsExpenditureReport.pdf> (accessed July 12, 2019).

Federal Fiscal Year	Date Received	Amount Received
2003	06/17/2004	$ 35,992,863
2004	06/17/2004	$ 64,585,966
2008	01/06/2009	$ 4,919,086
2009	02/01/2010	$ 4,277,466
2010	09/24/2010	$ 2,994,226
2011	03/16/2012	$ 52,202
Total		**$ 112,821,809**

Source: Produced by the Department of the Auditor General staff from the EAC website <https://www.eac.gov/payments-and-grants/managing-requirements-payments/> (accessed July 12, 2019).

In March 2018, the United States Congress provided states an additional $380 million of Section 251 funding through the Omnibus Appropriations Act of 2018. States could begin spending funds once they received their notice of grant award on April 17, 2018. As of September 30, 2018, Pennsylvania received $13,476,156 in grant funds, earned interest totaling $24,077, and had yet to expend the funds.[161] Pennsylvania plans to replace voting equipment that is reaching the end of its usable life with new equipment that has a voter verifiable paper audit trail.[162]

[161] The U.S. Election Assistance Commission, *Grant Expenditure Report Fiscal Year 2018*, dated April 4, 2019. <https://www.eac.gov/assets/1/6/FY2018HAVAGrantsExpenditureReport.pdf> (accessed July 12, 2019).
[162] Ibid.

Appendix G Description of Data Used in the Audit

The table below shows the number of records included in the Voter Table data obtained for this audit as of October 9, 2018. This table differs from the numbers included in *Appendix E*, which shows the number of registered voters by party, by county certified as of the November 6, 2018, election.

Status of Voter Records in the Voter Table as of October 9, 2018	
Number of Records	**Voter Status**
7,693,493	Active[a/]
874,207	Inactive[b/]
8,567,700	**Subtotal – Eligible to Vote**
7,789	Hold[c/]
16	Blank[d/]
7,495,963	Cancelled[e/]
16,071,468	**Total number of records in the voter table from the Statewide Uniform Registry of Electors (SURE) Database as of October 9, 2018**

[a/] An active voter is a person who is fully registered to vote.
[b/] An inactive voter is a person who is fully registered to vote but has not voted in at least five years, nor has had certain types of communication with their county election office. An inactive voter can vote once they complete an affidavit attesting to their eligibility to vote at that polling place.
[c/] A voter's registration can be placed on hold for several reasons, including imprisonment.
[d/] No status was included in the status field.
[e/] A voter whose registration has been cancelled will no longer be printed in the poll book and will not be able to vote until they re-register.

Source: This table was compiled by the staff of the Department of the Auditor General from data received from the Department of State that was extracted from the SURE system.

Appendix H SURE Survey

As part of our audit procedures, the following survey was sent on September 24, 2018, to the County Election Office Director in each of Pennsylvania's 67 counties. We requested that each director respond to the survey questions in order to assist us in gaining a comprehensive understanding of the Statewide Uniform Registry of Electors (SURE).

SURE Survey

County Name:

Name(s) and title(s) of individual(s) completing the survey:

General Questions

- How many people work on a daily basis processing voter registration related documents?
- Number of employees considered full time?
- Number of employees considered part time (approximate number of hours per week)?
- Of those employees, how many work in a supervisory/management position?
- How many precincts are in your county September 21, 2018?

Guidance/Training

1. Do you utilize the SURE Job Aids developed by DOS? ◯ Yes ◯ No

   Do you find them to be useful and/or sufficient? ◯ Yes ◯ No

   If you don't use the SURE Job Aids, why not?

2. How often do you generally utilize the SURE Help Desk?

   ○ Weekly
   ○ Monthly
   ○ Bi-annually
   ○ Annually
   ○ Don't use

   If you utilize the SURE Help Desk, what is it typically regarding?

3. Have you received other guidance from DOS or another source regarding registration and maintenance of your voter rolls? ◯ Yes ◯ No

   If yes, please describe.

2

4. Do you request SURE training from DOS for new employees? ◯ Yes ◯ No

   If no, how do you provide training to new employees?

5. Do you notify DOS when you hire a new employee? ◯ Yes ◯ No

6. Do you notify DOS when an employee leaves employment with the county? ◯ Yes ◯ No

Processing Applications

7. Do you review work completed in SURE by your employees to ensure that it is accurate? ◯ Yes ◯ No

   If yes,

   Who reviews (Please list the title of the reviewer)?

   How often?

   Is the review documented and maintained?

8. How does your office handle applications that you cannot initially register or deny?

9. If the HAVA check comes back without a match, do you:
   Reject without further investigation ○ Yes ○ No
   Conduct further investigation ○ Yes ○ No

   If further investigation is conducted, please provide explanation of additional work performed.

10. Do you scan and retain within SURE all paper voter registration applications? ○ Yes ○ No

    If no, why not?

    Do you retain the hard copy paper applications? ○ Yes ○ No

    If yes, for how long?

Poll Books

11. How do you print your poll books? ○ In-house ○ Contracted vendor

    If neither, please explain.

12. Do you have procedures in place to ensure that the printed poll books include all applicable records from SURE? ◯ Yes ◯ No

    If yes, please describe:

List Maintenance

13. Does your office conduct list maintenance as prescribed by state law (NCOA, 5 year mailings, etc.)? ◯ Yes ◯ No

    If yes, when is each type of maintenance activity conducted?
    NCOA
    Five year mailing
    Other list maintenance activities (please include the type of activity and approximate date activity is conducted)

14. Do you conduct a review to ensure that the required list maintenance activities have been completed and completed accurately? ◯ Yes ◯ No

    If yes,

    Who reviews (Please list the title of the reviewer)?

    How often is a review conducted?
    Is the review documented and maintained?

External reviews/audits

15. Has your office received any external reviews/audits (excluding DOS and the current Department of the Auditor General audit) of your operations related to voter registration or elections? ◯ Yes ◯ No

    If yes, who conducted the review/audit?

SURE Changes

16. Please provide your thoughts on issues within SURE and if you could recommend changes or additions to functionality what would they be?

IT Questions

17. Has your County connected any county-owned IT equipment to the SURE system (i.e., servers, printers, switches, monitors, keyboards, etc.)? ◯ Yes ◯ No

    If so, please list

18. Do County Election Workers or contractors share user IDs and passwords to the SURE system? ◯ Yes ◯ No

    If yes, why?

19. Do you periodically review SURE users to determine whether access is still appropriate? ◯ Yes ◯ No

    If yes, please describe:

20. Do you monitor security events and respond to security breaches in the IT equipment connected to the SURE system? ◯ Yes ◯ No

    If yes, please describe:

21. During the recent disaster recovery test of SURE in July 2018, were you able to log in and perform all the required tests successfully? ◯ Yes ◯ No

    Please list any tasks you were unable to perform:

22. Has anyone with access to the SURE system (employee or contractor) attended any cybersecurity awareness training since January 2016? ◯ Yes ◯ No

    If yes, please describe the training, including who conducted the training and who attended from the County:

23. Has anyone with access to the SURE system (employee or contractor) participated in cybersecurity awareness groups such as the Center for Internet Security's Multi-State Sharing and Analysis Center (MS-ISAC)? ◯ Yes ◯ No

    If yes, please describe the group and who attends:

24. DOS has recently developed the Online Voter Registration Web Application Programming Interface (PA OVR WEBAPI) to facilitate uploading large numbers of voter registration applications into SURE from outside organizations (i.e., voter registration drives). Has your office processed applications uploaded from the PA OVR WEBAPI? ◯ Yes ◯ No

    If yes, please describe any problems you may have encountered.

Please use the space below if additional space is necessary.

Appendix I Distribution List

This report was distributed to the following Commonwealth officials:

The Honorable Tom Wolf
Governor

The Honorable Kathy Boockvar
Secretary of the Commonwealth
Pennsylvania Department of State

The Honorable Jonathan Marks
Deputy Secretary for Elections
and Commissions
Pennsylvania Department of State

Mr. Timothy E. Gates
Chief Counsel
Pennsylvania Department of State

The Honorable John MacMillan
Deputy Secretary for Information
Technology and Chief Information
Officer
Office of Administration

The Honorable Garth Everett
Majority Chair
House State Government Committee

The Honorable Kevin Boyle
Democratic Chair
House State Government Committee

The Honorable Kristin Hill
Vice-Majority Chair
Senate State Government Committee

The Honorable Michaele Totino
Majority Executive Director
Senate State Government Committee

The Honorable Anthony Williams
Democratic Chair
Senate State Government Committee

The Honorable Jen Swails
Secretary of the Budget
Office of the Budget

The Honorable Joseph M. Torsella
State Treasurer
Pennsylvania Treasury Department

The Honorable Josh Shapiro
Attorney General
Office of the Attorney General

The Honorable Michael Newsome
Secretary of Administration
Office of Administration

Mr. William Canfield
Director
Bureau of Audits
Office of Comptroller Operations

Ms. Mary Spila
Collections/Cataloging
State Library of Pennsylvania

A Performance Audit

Pennsylvania Department of State
Statewide Uniform Registry of Electors

This report is a matter of public record and is available online at www.PaAuditor.gov. Media questions about the report can be directed to the Pennsylvania Department of the Auditor General, Office of Communications, 229 Finance Building, Harrisburg, PA 17120; via email to: News@PaAuditor.gov.

EXHIBIT 23

Wisconsin Elections Commission Memoranda, To: All Wisconsin Election Officials 3 (Aug. 19, 2020)

Wisconsin Elections Commission

212 East Washington Avenue | Third Floor | P.O. Box 7984 | Madison, WI 53707-7984
(608) 266-8005 | elections@wi.gov | elections.wi.gov

DATE: August 19, 2020

TO: All Wisconsin Election Officials

FROM: Meagan Wolfe, Administrator; Richard Rydecki, Assistant Administrator

SUBJECT: **Absentee Ballot Drop Box Information**

This document is intended to provide information and guidance on drop box options for secure absentee ballot return for voters. The information has been adapted from a resource developed as part of the Cybersecurity and Infrastructure Security Agency (CISA) Elections Infrastructure Government Coordinating Council and Sector Coordinating Council's Joint COVID Working Group. The original document can be found here: https://static1.squarespace.com/static/5a665c98017db2b60bc22084/t/5e8f42d717ee5e7ee2db8c8b/1586447064805/Ballot_Drop-Box_final.pdf.

What is an Absentee Ballot Drop Box?

A ballot drop box provides a secure and convenient means for voters to return their by mail absentee ballot. A drop box is a secure, locked structure operated by local election officials. Voters may deposit their ballot in a drop box at any time after they receive it in the mail up to the time of the last ballot collection Election Day. Ballot drop boxes can be staffed or unstaffed, temporary or permanent.

Some voters prefer to deliver their by mail absentee ballots to a drop box rather than sending them back through the mail. These voters may be motivated by lack of trust in the postal process, fear that their ballot could be tampered with, or concern that their information will be exposed. Voters may also be concerned about ensuring that their ballot is returned in time to be counted.

Ballot drop boxes and drop-off locations allow voters to deliver their ballots in person. More importantly, the availability of ballot drop boxes and drop-off locations ensures that even voters who wait until the last minute to return their ballot or who receive their requested ballot in the mail too late to return it via USPS will have timely options to return their ballots.

Repurposing Options

In a COVID-19 environment, creative solutions may be required. Your municipality may already have infrastructure set up for secure collection of payment and materials. Consider repurposing the following options as secure ballot drops:

Wisconsin Elections Commissioners
Ann S. Jacobs, chair | Marge Bostelmann | Julie M. Glancey | Dean Knudson | Robert Spindell | Mark L. Thomsen

Administrator
Meagan Wolfe

- Designate drop boxes or mail slots set up for taxes, mail and public utilities as secure ballot drop locations.
- Partnering with public libraries to use book and media drop slots for ballot collection.
- Partnering with businesses or locations that have already implemented social distancing practices, such as grocery stores and banks.

Many of these locations are already secure and located in places familiar to city residents. If you choose to do something similar, be sure to inquire about the security of these drops and identify how you can access ballots returned through these options. These locations should be marked with signage that clearly identifies the location as a ballot drop box and lists the final time ballots will be collected on election day. After the final election day pickup, clear signage should be placed at each drop site marking the location as "closed for ballot drop" and information regarding additional ballot return options and deadlines should be listed on these signs.

Types of Drop Boxes

Outdoor Options

1. Staffed, Temporary Drive-Through Drop Off

A drive-through drop-off location is an easy way to keep traffic flowing when demand for a ballot drop box is at its peak, especially on Election Day. This drive-through is typically set up in a parking lot or a street depending on the location.

The team staffing the site accepts ballots from voters as they pull through, depositing them directly into a ballot box. For voters who prefer placing the ballot directly into the box themselves, the portable ballot box is brought to the car window. In addition to the supplies listed below, you will need a team of at least two to three to support the drop-off site.

- Pop-up tent
- Table
- Chairs
- Ballot box
- Road signs
- Orange cones
- Flashlights
- High-visibility vests for workers
- Weather appropriate support— propane heater, rain gear, lanterns
- Personal protective equipment such as gloves, masks, and hand sanitizer as appropriate and in accordance with current CDC guidance

2. Unstaffed, 24-Hour Ballot Drop Box

In high-demand areas, installing a permanent ballot drop box—one that can be accessed by voters 24/7—is a good solution. These boxes should be constructed of durable material such as steel and be permanently cemented into the ground. This type of ballot drop box may cost as much as $6,000 each. Other options such as courier boxes are available from industrial supply companies and may be more affordable. In addition to purchasing the 24-hour box you will need:

- Video surveillance camera (or place the drop box in an area already covered by a security camera)
- Media storage device (for recorded video)
- Municipal decal or Election signage
- Extra keys for opening slot and access door
- Security seals

Indoor Option

Staffed or Unstaffed – Indoor Temporary Ballot Drop Box

When demand for a ballot drop box is low, a temporary ballot box located in a place such as the municipal clerk's office is a good solution. These boxes should be constructed of durable material and include a key or combination lock as well as a way to securely fasten the box to prevent it from being moved or tampered with. This type of box looks similar to the example pictured here. Staffed drop boxes can also be used at polling places on election day to collect absentee ballots from voters without having those voters wait in line in the voting area.

In addition to purchasing or renting the ballot box, you will need:

- Padlock and keys (if not included)
- Bike chain or some other way to fasten the box to prevent it from being removed (if not staffed)
- Security seals

Security

Ballot drop boxes must be secured and locked at all times. Only an election official or a designated ballot drop box collection team should have access to the keys and/or combination of the lock. In addition to locks, all drop boxes should be sealed with one or more tamper evident seals.
Ideally, unstaffed 24-hour drop boxes should be located in areas with good lighting and be monitored by video surveillance cameras. When this is not feasible, positioning the box close to a nearby camera is a good option. Also consider placing it in a high traffic area and inviting local law enforcement to make regular observations.

Try to place indoor drop boxes in locations where they can be monitored by a person in real time. When ballot boxes are unstaffed and not being monitored, the box should be securely fastened to a stationary surface or immovable object, such as a counter or wall, in a way that prevents moving or tampering.

Chain of Custody

- Chain of custody logs must be completed every time ballots are collected.
- All ballot collection boxes/bags should be numbered to ensure all boxes are returned at the end of the shift, day, and on election night.
- Team members should sign the log and record the date and time, security seal number at opening, and security seal number when the box is locked and sealed again.

Location

Ballot drop boxes should be placed in convenient, accessible locations, including places close to public transportation routes, near or on college campuses, and public buildings, such as libraries and community centers familiar to voters and easy to find. If there is time, getting input from citizens and community groups is recommended.

All drop box locations should be evaluated for:

- Security
- Lighting (well-lit 24 hours a day)
- High visibility
- Security cameras
- Accessibility
- Voter convenience
- Parking or drive-through options

How Many Drop Boxes Do You Need?

At a minimum, you should have a drop box at your primary municipal building, such as the village hall. Voters generally know the locations of these buildings and are already accustomed to voting or doing business there. Some other best practices include:

- Have one drop box for every 15,000–20,000 registered voters.
- Consider adding more drop boxes to areas where there may be communities with historically low absentee ballot return rates.
- Use demographic data and analysis to determine whether there should be a different formula for rural and urban locations (i.e., 1 for every 15,000 residents may be every mile in an urban are, but every 50 miles in a rural area).

EXHIBIT 24

Wisconsin Safe Voting Plan 2020 Submitted to the Center for Tech & Civic Life, June 15, 2020, by the Mayors of Madison, Milwaukee, Racine, Kenosha and Green Bay (Jun. 15, 2020)

Wisconsin Safe Voting Plan 2020
Submitted to the Center for Tech & Civic Life
June 15, 2020

The State of Wisconsin found itself in the midst of an historic election in April of 2020 when statewide elections occurred in the midst of the COVID-19 pandemic. These elections included not only the presidential preference vote, but also local races for city councils, county boards, school board, and mayors, a statewide election for a seat on the Wisconsin Supreme Court, and numerous district-wide school referenda.

Municipalities were required to make rapid and frequent adjustments to ensure compliance with the rapidly changing Supreme Court, Wisconsin Supreme Court, and Wisconsin Election Commission (WEC) rulings about the election. (The April 2020 Election may go down in history as the only election in which the Wisconsin Supreme Court and the US Supreme Court weighed in on the same day on how the election would be conducted.)

The shifting legal landscape was also complicated by the extraordinary lengths municipal clerks went to to ensure that both voting and election administration were done in accordance with prevailing public health requirements.

As mayors in Wisconsin's five biggest cities - Milwaukee, Madison, Green Bay, Kenosha, and Racine - we seek to work collaboratively on the two remaining 2020 elections (August 11th and November 3rd) to: safely administer elections to reduce the risk of exposure to coronavirus for our residents as well as our election officials and poll workers; identify best practices; innovate to efficiently and effectively educate our residents about how to exercise their right to vote; be intentional and strategic in reaching our historically disenfranchised residents and communities; and, above all, ensure the right to vote in our dense and diverse communities.

Table 1: Summary of Municipalities' Electorate Data, June 2020

	Green Bay	Kenosha	Madison	Milwaukee	Racine
Estimated Eligible Voters	71,661	73,000	213,725	430,000	56,000
Registered Voters	52,064	47,433	178,346	294,459	34,734
2020 Election Budget	$329,820	$205,690	$2,080,283	$2,986,810	$409,529

All five jurisdictions share concerns about how to best facilitate voter participation and limit exposure to coronavirus. All five jurisdictions spent all or most of the budgeted resources for all of 2020 on the extraordinary circumstances this Spring. If no plan is approved, it will leave communities like ours with no choice but to make tough decisions between health and the right to vote; between budget constraints and access to fundamental rights. The time that remains between now and the November Election provides an opportunity to plan for the highest possible voter turnouts in the safest possible ways.

We are collectively requesting a total of $6,324,527 as summarized in Table 3 below and detailed extensively in the plan.

Review of the April 2020 Election

The April 2020 election placed two sacred duties of cities in conflict: keeping our residents safe and administering free and fair elections. Since Wisconsin's elections are administered at the municipal level, each municipality was on its own to deal with these dynamics. Our Municipal Clerks and their staff are all remarkable public servants, who responded nimbly and effectively to marshal the resources needed to run these elections under exceedingly challenging circumstances. In this election, all five of our municipalities faced:

- Precipitous drop-offs of experienced poll workers;
- A scramble to procure enough PPE to keep polling locations clean and disinfected and to mitigate COVID-19 risk for election officials, poll workers, and voters;
- A never-before-seen increase in absentee ballot requests;
- High numbers of voters who struggled to properly submit required photo ID and/or provided insufficient certification of absentee ballot envelopes; and
- Voters who, understandably, were completely confused about the timeline and rules for voting in the midst of a pandemic and required considerable public outreach and individual hand-holding to ensure their right to vote.

See Table 2, below, for detailed data on all five municipalities' April 2020 absentee mail and in-person early voting experiences.

Table 2: Summary of Municipalities' Experiences in April 2020 Election

	Green Bay	Kenosha	Madison	Milwaukee	Racine
# of voters who requested absentee ballots for April election	15,509	16,017	89,730	96,712	11,615
# of absentee ballots successfully cast in April	11,928	13,144	77,677	76,362	9,570
# of absentee ballot requests unfulfilled due to insufficient photo ID	Unknown	Unknown	1,840	2.5%	Estimated hundreds
# of absentee ballots rejected due to incomplete certification	312	196	618	1,671	368
# of secure drop-boxes for absentee ballot return	1	2	3	5	1
# of days of early voting	12	10	19	14	13
Use curbside voting for early voting?	✔	✖	✔	✔	✔
# of voters who voted in-person early absentee	778	85	4,930	11,612	1,543
# of additional staff enlisted for election-related efforts	86	60	225	95	20
$ spent on PPE	$2,122	$13,000	$6,305	Unknown	Unknown
# of polling locations	2	10	66	5	14
Use drive-thru or curbside voting on Election Day?	✔	✖	✔	✔	✔

Comprehensive Election Administration Needs for 2020

In early June 2020, all five municipal clerks and their staff, with review and support from all five cities' Mayors and Mayoral staff, completed a detailed, multi-page template (attached) providing both data and information about the municipalities' election plans and needs. This Wisconsin Safe Voting Plan 2020 is based on that comprehensive information. All five of our municipalities recommend the following four strategies to ensure safe, fair, inclusive, secure, and professional elections in our communities for the remaining 2020 elections:

Recommendation I: Encourage and Increase Absentee Voting (By Mail and Early, In-Person)

1. Provide assistance to help voters comply with absentee ballot requests & certification requirements
2. Utilize secure drop-boxes to facilitate return of absentee ballots
3. Deploy additional staff and/or technology improvements to expedite & improve accuracy of absentee ballot processing
4. Expand In-Person Early Voting (Including Curbside Voting)

Recommendation II: Dramatically Expand Strategic Voter Education & Outreach Efforts, Particularly to Historically Disenfranchised Residents

Recommendation III: Launch Poll Worker Recruitment, Training & Safety Efforts

Recommendation IV: Ensure Safe & Efficient Election Day Administration

As detailed in this plan, our municipalities are requesting **a total of $6,324,567** to robustly, swiftly, comprehensively, and creatively implement these four strategic recommendations in each of our communities. That request is summarized as follows in Table 3, below, and detailed extensively in the remainder of this plan.

Table 3: Summary of Resources Needed to Robustly Implement All Four Recommendations

Recommendation	Green Bay	Kenosha	Madison	Milwaukee	Racine	Totals
Encourage and Increase Absentee Voting By Mail and Early, In-Person	$277,000	$455,239	$548,500	$998,500	$293,600	**$2,572,839**
Dramatically Expand Strategic Voter Education & Outreach Efforts	$215,000	$58,000	$175,000	$280,000	$337,000	**$1,065,000**
Launch Poll Worker Recruitment, Training & Safety Efforts	$174,900	$145,840	$507,788	$800,000	$181,500	**$1,810,028**
Ensure Safe & Efficient Election Day Administration	$426,500	$203,700	$40,500	$76,000	$130,000	**$876,700**
Totals:	**$1,093,400**	**$862,779**	**$1,271,788**	**$2,154,500**	**$942,100**	**$6,324,567**

Recommendation I: Encourage & Increase Absentee Voting By Mail and Early, In-Person

Of all the things that need to be done to ensure access and safety at the polls, this is perhaps the most important and timely. It is time, resource, and labor intensive but results in the voter being able to vote by mail or from the relative safety of their car or at a socially distanced and carefully planned early voting site.

Overview of Absentee Voting in Wisconsin

Before discussing our strategies and plans to encourage and increase absentee voting, both by mail and in-person, early voting, it's important to first understand the absentee voting context in Wisconsin.

There are two ways to vote early in Wisconsin: in-person and through the mail. Both are technically called "absentee voting," a phrase held over from a time when absentee voting required you to affirm that you were over 80, ill, or going to be out of the municipality on Election Day. Those requirements no longer exist in the statutes, and people can vote early, or absentee, for any reason. The April 2020 election saw dramatic increases in the number of absentee ballot requests over previous elections.

While for many regular voters, absentee voting - whether completed by mail or early, in-person - is a relatively easy process, our five cities understand that absentee voting does not work easily for all voters. Our communities of color, senior voters, low-income voters without reliable access to the internet, people with disabilities, and students all have legitimate concerns about the absentee voting process.

Voting absentee by mail has been complicated by the fairly recent imposition of state law requiring voters to provide an image of their valid photo ID prior to first requesting an absentee ballot. While this works relatively easily for voters who have valid photo IDs and the technology necessary to upload an image file of that valid ID into the state's myvote.wi.gov website, it does not work well or easily for other voters who do not have valid photo ID (complicated by closure of DMVs due to the pandemic), lack access to reliable internet (also complicated by coronavirus-related closures or reduced hours at libraries and community centers, leaving those residents without regular public internet access that our municipalities normally provide), those who don't have smart phones to take and upload photos, and those who need additional education about what constitutes a valid photo ID. (For example, countless voters in our municipalities attempted to submit "selfies" as valid photo ID. Explaining to them that this was not a valid form of photo ID and instructing them on how to properly submit valid ID took considerable staff time and resources.)

Once the absentee ballot is received, it must be completed correctly to be successfully cast, and there are numerous certification requirements on the absentee ballot envelope; if not correctly completed, the ballot could be rejected. Prior to this April's

election, very small numbers of voters had traditionally chosen to cast ballots by mail. Municipal clerks' offices simply were not prepared and do not have the staffing or technological resources needed to quickly process dramatically higher numbers of absentee ballot requests, troubleshoot problems, answer voter questions, provide information and to expedite the processing of thousands of received absentee ballots on Election Day.

In-person early absentee voting also poses challenges for voters and election administrators. While all of our communities had previously offered early voting locations and hours, April's election required election officials to creatively and quickly expand in-person early voting opportunities, including curbside voting, all while prioritizing necessary COVID-19 precautions.

As indicated by Table 4, below, all five of our municipalities are already experiencing dramatic increases in the number of voters requesting to vote absentee, compared to pre-pandemic, and must procure resources to enable voters in our communities to meaningfully access absentee voting.

Table 4: Absentee Ballots in All Municipalities as of June 2020

	Green Bay	**Kenosha**	**Madison**	**Milwaukee**	**Racine**
# of voters on permanent absentee list prior to 2/18/20	1,628	1,856	2,062	6,252	613
# of voters on permanent absentee list as of 4/7/20	4,306	3,469	8,665	23,374	2,684
# of voters who have already requested absentee ballots for August 2020	5,162	9,450	36,092	53,438	3,389
# of voters who have already requested absentee ballots for November 2020	4,859	9,123	34,164	50,446	3,204

We are committed to making voting accessible via mail, in-person prior to Election Day, and at the polls on Election Day. Particularly in the midst of a global pandemic when many voters are rightfully apprehensive about in-person voting, we want to ensure that voters in our communities know they have options and we are committed to conducting the necessary voter outreach and education to promote absentee voting and encourage higher percentages of our electors to vote absentee.

Increasing the number of voters who cast votes prior to Election Day minimizes the risk of spreading COVID-19 on Election Day from in-person contacts at our polling locations, and it reduces the chance for lines and delays in voting on Election Day.

The Wisconsin Election Commission (WEC) has approved a proposal to mail all registered voters absentee ballot request forms, which allows our five communities to focus on helping voters overcome the barriers to successfully returning those forms so they can obtain, and then successfully submit, their completed absentee ballots. This measure will provide absentee request information directly to voters, alleviating the need for municipalities to expend the cost to send the mailing. However, it is unclear how this measure will affect the workload of municipal clerks. Although the WEC has directed that the forms be returned to the WEC for entry, municipal clerks must still review each record, process, mail, record receipt and canvass each absentee ballot.

All of our municipalities anticipate continued large increases in absentee voting based on the April 2020 trends. Milwaukee, for example, anticipates that 80% of residents will vote absentee by mail for both the August primary and the November general election.

All five cities have identified numerous barriers to successful absentee voting, including: voters facing numerous challenges to successfully submitting valid photo ID; voters needing assistance complying with absentee ballot certification requirements, including obtaining the required witness signature on the absentee ballot return envelope; the labor-intensive process faced by all of our clerks' offices of processing absentee ballot requests; and U.S. Postal Service errors and mail delays. All of these are challenges for our municipalities in normal elections, but they are all compounded by the coronavirus pandemic, and made exponentially more difficult by the unprecedented volume of absentee voting requests. This puts tremendous strain on municipal election clerks and their staff.

Our five cities share the desire to assist as many residents as possible with casting ballots before Election Day, serving as the greatest opportunity we have to mitigate the spread of COVID-19 in our communities. We have identified several strategies to help voters in each of our communities overcome these barriers to successful absentee voting, both by mail and in-person early voting.

Overall, our five communities are requesting **$2,572,839** in resources related to enabling our municipalities to overcome these particular barriers and ensure that our voters can meaningfully access absentee voting, both by mail and in-person early voting. These strategies and resource needs are broken down into four distinct component recommendations, within the overall umbrella of increasing and encouraging absentee voting:

1. **Provide assistance to help voters comply with absentee ballot requests & certification requirements**

- **Green Bay:** The City would like to employ bilingual LTE "voter navigators" ($45,000) to help residents properly upload valid photo ID, complete their ballots and comply with certification requirements, and offer witness signatures. These voter navigators can assist voters prior to the elections and then also be trained and utilized as election inspectors. They would also like to utilize paid social media and local print and radio advertising to educate and direct voters in how to upload photo ID and how to request and complete absentee ballots. ($2,000) **Total: $47,000**

- **Kenosha:** The City would like to have Clerk's staff train library staff on how to help residents request and complete absentee ballots, would like to produce ($3,000) and mail ($26,200) a bilingual absentee ballot instruction sheet with all absentee ballots to increase correctly completed and submitted ballots. The City would like to hire a trainer for seasonal election workers, volunteers and poll workers. This employee would also coordinate assignments to polling locations, the early driver up voting site, the Clerk's office for assistance in processing, data entry and filing of absentee requests and the Absentee Board of Canvassers (approximately $50,000). The increase in absentee ballots due to COVID-19 has tremendously increased the workload of the department. In order to properly serve the citizens and voters additional LTE employees are needed (approximately $175,000). **Total: $254,200**

- **Madison:** Plans to hold curbside "Get your ID on File" events with the Clerk this summer utilizing volunteers or paid poll workers ($15,000) equipped with PPE (estimated $5,000) and digital cameras ($4,500) to capture voter ID images for voters who are unable to electronically submit their IDs to the Clerk's office. They also need large flags to draw attention to these curbside sites ($4,000). Would also like mobile wifi hotspots and tablets for all of these sites ($100,000) so voters could complete their voter registration and absentee requests all at once, without having to wait for staff in the Clerk's office to follow up on paper forms. (These mobile wifi hotspots, tablets, and flags, could all then be repurposed for early in-person voting closer to the election.) **Total: $128,500**

- **Milwaukee:** The City notes that the biggest obstacle to Milwaukee residents, particularly those in poverty, to applying for an absentee ballot in April was access to the internet and securing an image of their photo ID. To address this, the City will be promoting and utilizing Milwaukee Public Library branch staff ($90,000 for both elections) for 3 weeks prior to each election to assist any potential absentee voters with applying, securing, and uploading images of their valid photo ID. **Total: $90,000**

- **Racine:** The City will recruit and promote ($1,000), train ($3,000), and employ paid Voter Ambassadors ($8,000) who will be provided with both PPE and

supplies ($4,000) and set up at the City's community centers to assist voters with all aspects of absentee ballot request, including photo ID compliance. Due to the increase of absentee mailed requests the City of Racine will need an additional 2 full time staff members in the Clerk's Office in order to have a reasonable turn-around time for absentee requests ($100,000). Total: **$116,000.**

Total: $635,700

2. **Utilize Secure Drop-Boxes to Facilitate Return of Absentee Ballots**

Our five communities all share a desire to expand voters' ability to easily return absentee ballots to the municipality without having to rely on the postal service, since, after April's election, many voters are (rightfully) apprehensive that putting their completed ballot in the mail does not guarantee it will be received and counted by the municipality by statutory deadlines. Voters also need to have confidence that they are returning their completed absentee ballots into secure containers that are not at risk of tampering. All five cities need resources to purchase additional secure drop-boxes and place them at key locations throughout their cities, including libraries, community centers, and other well-known places, to ensure that returning completed ballots is as secure and accessible to voters throughout our cities as possible.

- **Green Bay:** The City would like to add secure (security cameras $15,000) ballot drop-boxes (approximately $900 each) at a minimum of the transit center and two fire stations, but if funding were available would also install secure drop boxes at Green Bay's libraries, police community buildings, and potentially several other sites including major grocery stores, gas stations, University of Wisconsin Green Bay, and Northern Wisconsin Technical College, in addition to the one already in use at City Hall. **Total: $50,000**
- **Kenosha:** The City currently has two drop-boxes that are checked throughout the day, and would like to install 4 additional internal security boxes at Kenosha libraries and the Kenosha Water Utility so that each side of town has easy access to ballot drop-boxes. **Total: $40,000**
- **Madison:** The City would like to have one secure drop box for every 15,000 voters, or 12 drop boxes total ($36,000). The City would also like to provide a potential absentee ballot witness at each drop box, utilizing social distancing and equipped with PPE (staff costs unknown): **Total: $50,000**
- **Milwaukee:** The City would like to install secure 24-hour drop boxes at all 13 Milwaukee Public library branches, staffed with socially distanced volunteers to serve as witnesses. **Total: $58,500**

- **Racine:** The City currently has one secured drop box for absentee ballots, and would like to have 3 additional drop boxes, each equipped with security cameras, to install at key locations around the City. **Total: $18,000.**

Total: $216,500

3. **Deploy Additional Staff and/or Technology Improvements to Expedite & Improve Accuracy of Absentee Ballot Processing**

The process of assembling and mailing absentee ballots is labor-intensive, slow, and subject to human error. Absentee ballot requests must be approved and entered into the statewide system, labels must be printed and applied to envelopes, ballots must be initialled, folded, and inserted into the envelope along with instructions. Ballots must be logged when received back from the voter. Undeliverable ballots must be reviewed, reissued or canceled. When voters make mistakes on ballots the requests to reissue must be completed. These tasks are time-consuming and utilizing existing clerk's office staff pulls them away from all of the other service requests, phone answering, and tasks handled by busy municipal clerks' offices.

The tremendous increase in absentee ballot requests in April was unprecedented, and municipal clerks and their staff were unprepared for the volume. They responded remarkably well - particularly since many of their staff were, by late March and early April, working remotely or, at a minimum, all needing to adhere to social distancing and masking precautions when working together in the same room - but all five municipalities need additional resources to accurately and swiftly process absentee ballot requests.

- **Green Bay:** The City needs 45 additional staff to process absentee ballot requests before the election, to open and verify envelopes on Election Day, and insert them into the tabulators. After the election, staff are needed to enter new voter registrations and assist with all election certification tasks ($140,000 for staffing) The City would also like to purchase a ballot opener and ballot folder to expedite processing ($5,000). **Total: $145,000.**
- **Kenosha:** The City needs resources for absentee ballot processing, to staff and process early, in-person absentee requests, and to answer voters' questions (approximately $100,000). Additional workers are also needed to canvass absentee ballots (approximately $11,000) **Total: $111,000**
- **Madison:** Based on data from April, the City estimates it will need additional staffing ($110,000) for hourly election clerks for the fall elections, and will incur

additional overtime costs ($100,000) for staff processing of absentee ballots and other election-related tasks. **Total: $210,000**

- **Milwaukee:** Given its tremendous volume of absentee ballot requests and processing tasks which far exceeds that of the other municipalities, Milwaukee would like to completely automate and expedite the assembly and mailing of requested absentee ballots. The City would like to purchase a high-speed, duplex printer, a top-of-the-line folding machine, and a high quality folding and inserting machine. This would reduce staff costs and eliminate the use of absentee labels, by enabling the City to print directly onto inner and outer envelopes. This would also allow the City to have a small 2D barcode that the inserter machine would be able to scan to ensure that the outer envelope is for the same voter; increasing quality controls. This automation would enable the City to eliminate the assembly delay no matter the volume of daily absentee requests, allowing experienced election workers and previously trained election temporary employees to be re-deployed to early voting sites as supervisors and lead workers. **Total: $145,000**

- **Racine:** To process absentee ballot requests in April, the City estimates that it will need seven additional full-time employees to process fall election requests. These employees will be needed full-time for one month prior to the August Election (approximately $17,000) and seven weeks prior to the November election (approximately $30,000). **Total: $47,000**

Total: $658,000

4. **Expand In-Person Early Voting (Including Curbside Voting)**

For a variety of reasons, many voters in our municipalities do not want to vote by mail and prefer to vote in-person. As a result of the coronavirus, far more voters are interested in early, in-person absentee voting (EIPAV) than we've seen in previous elections, wishing to avoid lines or crowds on Election Day. All five municipalities would like to have resources to accommodate these early, in-person voters. Expanding access to early, in-person voting also will lessen lines at polling places on Election Day and allow for proper social distancing and other pandemic precautions to be uniformly implemented.

Curbside and drive-thru voting have been very popular with residents of our municipalities, particularly for those with health concerns who can remain in the cars and have a virtually contact-less voting process. For example, Milwaukee previously operated in-person early voting for one week leading up to the April election at three sites and then transitioned to one site of drive-thru voting. 11,612 cast ballots through these options: 5,571 via in-person and 6,041 at drive-thru, and these numbers represent a 46% increase over April 2016 "early voting" totals. However, it is slow-moving and

labor-intensive. Additionally, particularly in the larger cities among us, it requires law enforcement and traffic control assistance to help manage traffic.

- **Green Bay:** The City would like to expand and establish at least three EIPAV sites in trusted locations, ideally on the east (potentially UWGB) and west sides (potentially NWTC or an Oneida Nation facility) of the City, as well as at City Hall. The City is planning to offer early voting starting two weeks before each election, with several weekdays available until 6:30pm and Saturdays 10am-4pm. They would like to staff these early voting sites with election inspectors who are bilingual and would like to increase the salary rate for these bilingual election inspectors to assist with recruitment and retention, as well as in recognition of their important role at these sites. The City also will need to print additional ballots, signage, and materials to have available at these early voting sites. **Total: $35,000.**

- **Kenosha:** The City plans to have one early voting location, at City Hall, and plans to hold early voting two weeks before the August election, with no weekend or evening hours planned, and 4 weeks before the November election, with access until 7pm two days/week and Saturday voting availability the week before the election. If City Hall is still closed to the public, they will explore offering early drive thru voting on City Hall property. Resources are needed for staffing (approximately $40,000), PPE ($1,050), signage ($200), laptops, printers, and purchase of a large tent ($8,789) to utilize for drive thru early voting. Staff could see voters' ID, print their label, hand them their ballot, and then collect the completed envelope. This would also allow staff to help voters properly do certification and provide witness signatures if necessary. The City could do this for one full week before elections. **Total $50,039.**

- **Madison:** The City would like to provide 18 in-person absentee voting locations for the two weeks leading up to the August election, and for the four weeks leading up to the November election. Their original plan was to offer in-person absentee voting at all nine library locations, the City Clerk's Office, a city garage, Edgewood College, two Madison College locations, and four UW-Madison locations. Due to weather uncertainties, they will need to purchase and utilize tents ($100,000) for the curbside voting locations in order to protect the ballots, staff, and equipment from getting wet and will also need large feather flags to identify the curbside voting sites. (Additional staff costs covered by the earlier question re. Absentee ballot processing.) The City would also like to get carts ($60,000) for our ExpressVote accessible ballot marking devices so we can use the ExpressVote for curbside voting to normalize the use of ExpressVote to help voters with disabilities feel less segregated during the voting process.**Total: $160,000.**

- **Milwaukee:** The City would like to set up 3 in-person early voting locations for two weeks prior to the August election ($150,000) and 15 in-person early voting

locations and 1 drive-thru location, potentially at a central location like Miller Park, for four weeks prior to the November election ($450,000). (Establishing this many EIPAV sites requires a significant investment in IT equipment, an additional ballotar printer, tents, signage, and traffic control assistance. Milwaukee would also like to offer evening and weekend early voting hours which would add additional costs for both August ($30,000) and November ($75,000). **Total: $705,000.**

- **Racine:** The City would like to offer a total of 3 EIPAV satellite locations for one week prior to the August election, as well as offering in-person early voting - curbside, if City Hall is still closed to the public - at the Clerk's office for 2 weeks prior to the August election. For the November election, Racine would like to offer EIPAV at 4 satellite locations two weeks prior to the election and at the Clerk's office (again, potentially curbside) 6 weeks prior. The City would need to obtain PPE, tents, supplies and cover staff time and training ($40,000). Racine would also like to have all satellite locations available for half-day voting the two Saturdays ($17,000) and Sundays ($17,000) prior to the November election, and the library and mall locations would be open until 8pm the week prior to the Election. Additional resources needed include one-time set-up fee per location ($7,500), laptops and dymo printers ($10,000), training ($1,100), and signage ($12,000.) As well, the City would like to host at least one drive-thru Voter Registration Day, where City Hall would be set up for residents to come get registered, curbside, and get their voting questions answered by Clerk's staff. Newly registered voters could also get assistance requesting absentee ballots for upcoming elections while they're there. ($8,000) **Total: $112,600**

Total: $1,062,639.00

Recommendation I Total for All Strategies to Encourage and Increase Absentee Voting by Mail and Early, In-Person: $2,572,839.00

Recommendation II: Dramatically Expand Voter & Community Education & Outreach, Particularly to Historically Disenfranchised Residents

All five municipalities expressed strong and clear needs for resources to conduct voter outreach and education to their communities, with a particular emphasis on reaching voters of color, low-income voters without reliable access to internet, voters with disabilities, and voters whose primary language is not English. This outreach is particularly necessary given the voter confusion that ensued in the lead-up to the April election, and voters' concerns and questions about voting during the COVID-19 pandemic. We understand that our communities of color do not necessarily trust the voting process, and that we need to work to earn that trust. We want to be transparent and open about what happens behind the scenes in elections, and what options are available for casting a ballot. We also want to make sure we are listening to groups that have historically been disenfranchised and groups that are facing obstacles with voting during this pandemic, and working with them to effectively respond to their concerns.

Voter outreach and education is also needed to encourage and explain new voter registration, and to encourage voters to verify and update their address or other voter registration information to do so prior to the Election. None of our communities have sufficient resources budgeted or available for the strategic, intentional, and creative outreach and education efforts that are needed in our communities over the summer and into the fall.

We all want our communities to have certainty about how the voting process works, trust in our election administration's accuracy, and current, accurate information on what options are available to vote safely in the midst of the pandemic. Significant resources are needed for all five municipalities to engage in robust and intentional voter education efforts to reduce confusion; encourage and facilitate new voter registration and registration updates; provide clear, accessible, and accurate information; address voters' understandable pandemic-related safety concerns; reassure voters of the security of our election administration; and, ultimately, reduce ballot errors and lost votes and enhance our residents' trust and confidence in our electoral process.

- **Green Bay:** Would like to reach voters and potential voters through a multi-prong strategy utilizing "every door direct mail," targeted mail, geo-fencing, billboards, radio, television, and streaming-service PSAs, digital advertising, and automated calls and texts ($100,000 total). The City would also like to ensure that these efforts can be done in English, Spanish, Hmong, and Somali, since roughly 11% of households in the Green Bay area speak a language other than English. Ideally, the City would employ limited term communications staff or engage communications consultants ($50,000) from August through the November election to design these communications and design and launch paid advertising on Facebook, Twitter, and Instagram, also in multiple languages. The City would also like to directly mail to residents who are believed to be eligible but not registered voters, approximately 20,000 residents. It would require both

considerable staff time to construct that list of residents and directly mail a professionally-designed piece (in multiple languages) to those voters. ($50,000 total for staffing, design, printing, and postage). To assist new voters, the City would also like resources to help residents obtain required documents (i.e. birth certificates) which are needed to get a valid state ID needed for voting. These grant funds ($15,000) would be distributed in partnership with key community organizations including churches, educational institutions, and organizations serving African immigrants, LatinX residents, and African Americans.
Total: $215,000

- **Kenosha:** Would like to directly communicate to all Kenosha residents via professionally-designed targeted mail postcards that include information about the voter's polling location, how to register to vote, how to request an absentee ballot, and how to obtain additional information. The City would have these designed by a graphic designer, printed, and mailed ($34,000). The City would also like resources for social media advertising, including on online media like Hulu, Spotify, and Pandora ($10,000) and for targeted radio and print advertising ($6,000) and large graphic posters ($3,000) to display in low-income neighborhoods, on City buses, and at bus stations, and at libraries ($5,000).
Total: $58,000

- **Madison:** Would like to engage the City's media team to produce videos to introduce voters to the election process, voting options, and to explain the safety precautions taken at polls and early voting sites. These videos would then be shared in numerous ways, including through partner organizations and on the City's social media platforms. The City would also like to partner with community organizations and run ads on local Spanish-language radio, in the Spanish-language newspapers, on local hip hop radio stations, in African American-focused printed publications, and in online publications run by and for our communities of color (advertising total $100,000). Additionally, the City has many poll workers who are from historically disenfranchised communities. The City would like to pay those poll workers ($75,000) to conduct voter outreach and additional poll worker recruitment activities. **Total: $175,000.**

- **Milwaukee:** Would like to partner with other City divisions to develop mailings and door hangers ($10,000) that could accompany water bills, be distributed by the Department of Neighborhood Services, or hung on trash receptacles by sanitation staff. The City would also like to revamp current absentee voting instructions to be more visual, address issues specific to the pandemic such as securing a witness signature, prepare it in English and Spanish, and print 150,000 color copies (estimated total $15,000). The Election Commission would also like to produce a short video ($5,000) with visuals showing voters how to apply for an absentee ballot and how to correctly complete and return the ballot. Additionally, the Election Commission would like to hire a communications firm to prepare and implement a comprehensive voter outreach communications plan

($250,000). This communications effort would include numerous voter education ads and PSAs on radio, billboards, buses, with some using local celebrities like Milwaukee Bucks players. This communications effort would focus on appealing to a variety of communities within Milwaukee, including historically underrepresented communities such as LatinX and African Americans, and would include a specific focus on the re-enfranchisement of voters who are no longer on probation or parole for a felony. Additionally, this campaign would include an edgy but nonpartisan and tasteful communications campaign to harness the current protests' emphasis on inequity and ties that message to voting. The video, the ads, and the PSAs could all also be placed on social media, the Election Commission and City websites, and GOTV partner websites and social media. **Total: $280,000**

- **Racine:** The City would like to retain a communications firm to design and implement a comprehensive voter outreach communications plan ($80,000). This would include ads on Facebook, Instagram, and Snapchat. The City would also like to rent billboards in key parts of the City ($5,000) to place messages in Spanish to reach Spanish-speaking voters. The City would also like to do targeted outreach aimed at City residents with criminal records to encourage them to see if they are not eligible to vote; this outreach will be accomplished with the production, editing, and sharing of a YouTube video ($2,000) specifically on this topic shared on the City's website, social media channels, and through community partners. Racine would also like to purchase a Mobile Voting Precinct so the City can travel around the City to community centers and strategically chosen partner locations and enable people to vote in this accessible (ADA-compliant), secure, and completely portable polling booth on wheels, an investment that the City will be able to use for years to come. (Estimated cost $250,000). **Total: $337,000**

Recommendation II Total For All Strategies to Dramatically Expand Strategic Voter Education and Outreach Efforts, Particularly to Historically Disenfranchised Residents: $1,065,000.00

Recommendation III: Launch Poll Worker Recruitment, Training, and Safety Efforts

The pandemic made conducting Election Day activities extremely challenging. Most poll workers in Wisconsin are retirees doing their civic duty to help facilitate the election. Given the increased risk for the elderly if exposed to COVID-19, many experienced poll workers opted out. Milwaukee had so many poll workers decline to serve that the City went from 180 polling locations to five polling locations. Green Bay, facing a similar exodus of poll workers, went down to two polling locations. Racine usually relies on nearly 190 poll workers for a spring election; only 25 of those experienced poll workers were under the age of 60.

As fears about the coronavirus increased in mid-late March and early April, poll workers in all five municipalities declined to work the election, leaving cities scrambling to quickly recruit enough bodies to keep polling locations open. All cities were appreciative of the last minute assignment of hundreds of Wisconsin National Guard members to assist with Election Day activities, and all of our cities re-assigned City staff from other departments to serve as poll workers and election officials and to assist with the myriad of tasks related to Election Day administration. The remainder of positions were staffed by high school students, college students, and members of the National Guard. Many of our poll workers had never worked an election before.

- **Green Bay:** The City needs to hire a total of 380 workers per election (total $112,660). The City would like to pay poll workers more than they have previously received, to signify their importance in the process and to acknowledge the extra challenge it represents to serve as an election official during a pandemic. The City would like to increase poll worker salaries by 50% (additional $56,330). All poll workers will be trained through the Wisconsin Elections Commission website and the City's own training manual ($6,000). **Total: $174,900**

- **Kenosha:** The City needs to hire 350 poll workers per election ($100,000). They would like to offer hazard pay to increase pay to $160/worker and $220/chief inspectors ($10,840). To aid in recruitment efforts, the City would like to hire a recruiter and liaison position for poll workers ($35,000). **Total: $145,840.**

- **Madison:** The City utilizes the election toolkit available through the MIT Technology Project to determine the staffing levels needed to ensure that voters will not have to wait in line for more than 15 minutes. In addition to the one Chief Inspector per polling location, Madison also has additional election officials who are certified as the Absentee Lead at each polling location. Madison estimates that if 75% of votes cast are absentee, the City will need 1,559 election officials at the polls in August. The City envisions a robust and strategic poll worker recruitment effort, focusing on people of color, high school students, and college students. The City would like to have resources for hazard pay for poll workers this fall at a rate comparable to what the U.S. Census is paying in the area

($369,788). The City has also found it challenging to convince facilities to host a polling location in the midst of a pandemic, and would like to provide each facility with a small amount of funds to compensate for their increased cleaning and sanitization costs ($750/location, $138,000 total). **Total: $507,788**

- **Milwaukee:** The City plans to have 45 voting locations in August and to keep open as many of the normal 180 polling places as possible in November. August will require 3 chief inspectors per site and 20 election workers per site, for a total of 1200 election workers minimum and 150 chief inspectors. The City has a goal of recruiting 1,000 new election workers. The City would like to add an additional $100 per worker in hazard pay to the poll workers' stipends of $130 ($460,000 additional for both elections) and $100 hazard pay to chief inspector stipends of $225 ($87,750 additional for both elections). Additionally, the City of Milwaukee utilizes a Central Count of absentee ballots, which necessitates 15 chiefs and 200 election workers per election at Central Count ($50,000/day for 2- days each election for a total of $200,000). Total payroll for both elections will reach $750,000 based upon these calculations.The City will launch a recruitment campaign for a new generation of election workers to sign up and be involved in their democracy, and hopes this effort can be included in the above request for resources for a marketing firm. Recruiting new and younger poll workers means that the Election Commission will need to innovate in election training. The Commission would like to produce polling place training videos ($50,000) with live small-group, socially distanced discussions and Q&A sessions. These videos will augment existing training manuals. **Total: $800,000**

- **Racine:** The City needs approximately 150 poll workers for August and 300 for November, in addition to 36 Chief Inspectors, and would like to pay all workers a $100/election hazard pay ($118,000 total payroll for both elections). City notes that its desire to have more early voting locations and hours is directly impacted by its ability to hire and train election officials. To that end, the City would like to launch a recruitment campaign that includes radio ads ($1,000), ads on social media platforms ($10,000), billboards in strategic City locations ($5,000), and film videos for high school students in history/government classes ($500). The City would also like to enlist a communication firm to: create a training video for election officials, develop an online quiz, detailed packets for election officials, and a PPE video filmed by a health professional about necessary COVID-19 precautions during all voting operations ($22,000 total). Racine would also like to hire a liaison position to schedule, training and facilitate poll workers. ($35,000) **Total: $181,500.**

Recommendation III Total for All Strategies to Launch Poll Worker Recruitment, Training and Safety Efforts: $1,810,028.00

Recommendation IV: Ensure Safe & Efficient Election Day Administration

It is no small task to mitigate risk of a lethal pandemic at all polling locations and throughout all required Election Day processing. Municipal clerks must ensure they have done everything possible to comply with public health guidelines and mitigate the risk of COVID-19 for all of the election officials, poll workers, observers, and voters. Our five municipalities are in need of numerous resources to both ensure seamless processing of voters on the upcoming Election Days, procure Personal Protective Equipment (PPE), disinfectant, and cleaning supplies to protect election officials and voters from the coronavirus, and to aid in processing of an expected high volume of absentee ballots. Additionally, as several of our municipalities move to add or expand drive-thru voting on Election Days, those expansions come with additional unbudgeted expenses for signage, tents, traffic control, publicity, and safety measures. All of our municipalities need resources to ensure that the remaining 2020 Election Days are administered seamlessly and safely.

- **Green Bay:** Green Bay would like to purchase 135 electronic poll books ($2,100/each for a total of $283,500) to reduce voter lines, facilitate Election Day Registrations and verification of photo ID. The City would also like a high speed tabulator ($62,000) to count absentee ballots on Election Day, a ballot opener and ballot folder ($5,000), and additional staff to process absentee ballots on Election Day ($5,000). The City also needs masks, gloves, gowns, hair nets, face shields ($15,000), cough/sneeze guards ($43,000), and disinfectant supplies ($3,000). **Total: $426,500**

- **Kenosha:** The City would like to purchase automatic hand sanitizer dispensers for all polling locations ($14,500) as well as PPE (gloves, masks, disinfectant, etc.) for all poll workers and voters ($15,200). Kenosha would also like to be able to offer elderly residents and people with disabilities who wish to vote in person on Election Day two-way transportation, utilizing a local organization such as Care-A-Van ($2,000). The City also needs resources for technology improvements to include a ballot opener, a ballot folder, 12 additional laptops and dymo printers, and high-speed scanner tabulators ($172,000 total) to expedite election day processing and administration. **Total: $203,700**

- **Madison:** The City needs hand sanitizer for all poll workers and voters, disinfectant spray, plexi-glass shields to allow poll workers to split the poll books, face shields for curbside election officials, and face masks for all poll workers and observers ($20,000) as well as renting additional space to safely and accurately prepare all supplies and practice social distancing at the public test of election equipment ($20,000) If the new voter registration form is not translated by the state into both Spanish and Hmong, Madison plans to translate the form ($500). **Total: $40,500**

- **Milwaukee:** The City will be purchasing 400 plexiglass barriers ($55,000) for election workers at all polling location receiving and registration tables. Additionally, the Milwaukee Election Commission will need to acquire 400 face shields for workers not staffed behind plexiglass ($4,000), gloves for all poll workers ($3,000), masks on hand for election workers and members of the public ($5,000), hand sanitizer ($2,000) and disinfectant ($2,000). Additionally, since Milwaukee also plans to offer curbside voting as an option at all polling places, updated, larger, more visible signage is necessary ($5,000). **Total: $76,000**

- **Racine:** Racine plans to issue all 36 wards its own PPE supply box which will each include masks, cleaning supplies, pens for each voter, gloves, hand sanitizer, safety vests, goggles, etc. ($16,000). The City also needs large signs to direct and inform voters printed in English and Spanish ($3,000). Additionally, the City would like to deploy a team of paid trained EDR Specialists for each polling location ($10,000, including hourly pay, training expenses, and office supplies). As well, Racine would like iPads with cellular signal for each polling location to be able to easily verify voters' registration status and ward ($16,000). The City would like to equip all wards with Badger Books ($85,000); Racine began using electronic poll books in the February 2020 election and has found they dramatically increase and facilitate EDR, verification of voters' photo ID, expedite election processes, and reduce human error. **Total: $130,000**

Recommendation IV Total for All Strategies to Ensure Safe & Efficient Election Day Administration: $876,700.00

Conclusion

As Mayors in Wisconsin's five largest cities, we are committed to working collaboratively and innovatively to ensure that all of our residents can safely exercise their right to vote in 2020's remaining elections in the midst of the COVID-19 pandemic. The April 2020 election placed two of our most sacred duties in conflict: keeping our residents safe and administering free, fair, and inclusive elections. This Wisconsin Safe Voting Plan 2020 represents a remarkable and creative comprehensive plan, submitted collaboratively by all five of our cities. With sufficient resources, all five municipalities will swiftly, efficiently, and effectively implement the recommended strategies described in this plan, to ensure safe, fair, inclusive, secure, and professional elections in all of our communities this year.