



U. S. ELECTION ASSISTANCE COMMISSION
VOTING SYSTEM TESTING AND CERTIFICATION PROGRAM
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

October 1, 2020

Sent via e-mail

Re: ExpressVote 1.0 Trusted Build

Dear State Election Directors,

On September 23, 2020, the U.S. Election Assistance Commission (EAC) was notified by the Texas Secretary of State's (SOS) office that they discovered a hash value discrepancy with a voting system they were examining for certification, ES&S EVS 6.0.3.0. This hash value discrepancy was discovered on ExpressVote 1.0 when the Texas SOS staff exported the software files from the installation USB drive and the installation files from the trusted build and imported them into a 3rd party software tool, Ubuntu, which compared the two hash values and displayed the mismatched hash value.

It's important to note in this case that the states and their jurisdictions wouldn't have seen an automated hash value error displayed on the screen as there are two separate load processes, which makes it impossible to allow for the system to compare the two hashes and display an error message. Discovering the hash value discrepancy would require a manual process of comparison by reviewing the hash value from the Inno disk (inside the unit) which loads the entirety of the installation (all files), to the hash value from the USB drive (as it only loads the firmware).

Texas SOS representatives and ES&S representatives determined this validation error existed in EVS 6.0.2.0 as well. Both versions are certified by the EAC to VVSG 1.0 and EVS 6.0.2.0 is currently deployed in 43 counties in Texas. 18 of the 43 counties use a configuration of EVS 6.0.2.0 that includes the ExpressVote 1.0.

As part of EAC certification, manufacturers are required to submit system identification tools and procedures that use hashes to prove that the applications installed on a voting system exactly match the certified versions. ES&S explained that only one file was causing the hash validation error, a bitmap image file (SYSLOAD.BMP) with a copyright date that displays on the ExpressVote while booting up. ES&S further explained that the issue occurs only if a USB update method is used to update the version of the ExpressVote unit from a previous version. The reason the update method causes the issue is due to the fact that the USB drive is a quick installation method that is designed to ONLY update firmware, and because the bitmap file is not part of the firmware, the installation via the USB drive method didn't replace the bitmap file and left the old bitmap file on the system resulting in the hash discrepancy.

Texas contracted with the voting system test laboratory (VSTL) Pro V&V to verify ES&S' claim that the SYSLOAD.BMP file was the only change to the certified trusted build. Pro V&V performed a source code comparison of the EVS 6.0.2.0 update image disk file and the EVS 6.0.2.0 production release disk image file. Pro V&V confirmed that the only change was a bitmap file. Pro V&V upgraded an ExpressVote from EVS 5.2.2.0 to EVS 6.0.2.0, received a hash mismatch message as expected, and

performed functional testing on the upgraded ExpressVote. Pro V&V concluded that the hash mismatch error does not impact the functionality of the ExpressVote. Pro V&V's test report is attached to this letter.

Initially, we were under the impression that only EVS 6.0.2.0 systems in Texas were impacted. We requesting information from ES&S to better understand the scope and to date have received information that the states listed in Table 1 have at least one jurisdiction that may be affected. Please note that this information is current as of October 1, 2020. We will provide updated information as soon as it is received.

Table 1

State	# of Units	Status
AL	105	Potentially affected
AR	2072	Potentially affected
AZ	496	Potentially affected
DC	102	Affected
FL	2893	Potentially affected
IA	532	Potentially affected
ID	346	Potentially affected
IN	731	Potentially affected
KS	1742	Potentially affected
KY	400	Affected
MD	3501	Likely unaffected
MI	548	Potentially affected
MO	538	Potentially affected
OH	168	Potentially affected
TN	671	Potentially affected
WA	3	Potentially affected
WI	667	Potentially affected
WY	20	Potentially affected

On September 29, 2020, we sent the following request to ES&S:

“In order to be in compliance with our Testing and Certification Program, we are requesting the following information. We may request additional information, and expect that you will disclose any other information that would assist us in understanding the scope of impact of any ES&S voting system regarding compliance with EAC certification.

1. The total number of jurisdictions throughout the United States affected including the jurisdiction name, contact information, and a list of affected devices including the system version information as well as serial numbers in each jurisdiction and when the installation occurred by ES&S personnel.

2. A detailed document providing a timeline of when this issue was first known and what ES&S is doing to remediate the issue.
3. All communication with the VSTLs regarding this issue.
4. An advisory notice specifying each EAC-certified voting system that uses the ExpressVote 1.0 and the ExpressVote's certified hashes and the mismatched hashes generated from the "update" file that has been installed on fielded devices.
5. All communication to the affected jurisdictions must represent the real facts regarding the circumstances.
6. Submit all documentation that supports your position regarding what you feel occurred.
7. A detailed document describing why ES&S disagrees with some of the statements the Texas Secretary of State's office made in their letter to ES&S dated September 24, 2020.
8. ES&S' plan to install EAC-certified software on the affected ExpressVotes in Texas.
9. ES&S' plan to install EAC-certified software on affected ExpressVotes as requested by jurisdictions.
10. ES&S' planned resolution, including a documented procedure, to ensure that this does not occur again.
11. ES&S' communication plan and any other documentation (timeline, FAQs) that will be distributed to the affected jurisdictions for review and approval by the EAC.
12. ES&S will communicate directly with the Executive Director or her designated representative and will cease to contact EAC employees throughout the duration of this investigation.

Finally, according to Section 5.15.4 of the Testing and Certification Program Manual, a manufacturer has 15 days from receipt of this letter to comply with the recommended corrective actions. However, due to the urgent nature of this issue and its impact on fielded, EAC-certified voting system 35 days before the 2020 General Election, we are requesting this information by close of business on October 1, 2020. We anticipate you immediately provide a written advisory of the situation to the states and localities impacted by this issue. We are requesting you utilize additional personnel and expend whatever resources necessary to install to provide an appropriate validated hash on identified EAC certified voting systems, resolving the issue upon request of the states. The EAC anticipates that we will review and re-test the software with incorrect hash validation in our accredited laboratories in the coming days and weeks. We anticipate your cooperation with this matter and working with the states and localities using the identified systems.

ES&S needs to be prepared to cooperate with the labs and EAC to provide complete test reports on each of the builds of different versions among the states that have an incorrect hash validation - so we have a complete record of testing results that confirms there is not any impact to accuracy, functionality, use, etc.

Failure to comply will result in the EAC taking immediate required action as it deems appropriate as the system no longer complies with its original certification, including but not limited to initiating decertification actions and/or suspension of manufacturer registration.

We are taking this matter very seriously and understand that ES&S does as well and appreciate a prompt response given the nature of this issue."

We will request that ES&S submit all update image files and voting system configurations to VSTLs for examination via our de minimis change process. Table 2 displays all affected EVS voting systems, firmware versions, and hash values of the production trusted build.

Table 2

EVS Release	FW Version	Copyright YRS	Hash Value
FL EVS 4500v4	1.2.3.0	2011 - 2013	f67dbc52fe9c5e65ad786740ca07388e864fc00aaabcb6e0169b44c485356101
EVS 5200 EVS 5300 EVS 5303 IL EVS 5300 EVS 5201 EVS 5202 EVS 5203 EVS 5204	1.4.0.0	2011 - 2014	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
EVS 5210 EVS 5310	1.4.1.0	2011 - 2015	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
EVS 5211	1.4.1.1	2011 - 2016	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
EVS 5220 EVS 5320	1.4.1.2	2011 - 2016	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
EVS 5321 EVS 5230 EVS 5330	1.4.1.6	2011 - 2017	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
EVS 5240 EVS 5340 EVS 5241 EVS5341	1.4.1.7	2011 - 2018	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
FL EVS 4520v1	1.4.2.0	2011 - 2015	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
FL EVS 4530v1	1.4.3.0	2011 - 2017	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
FL EVS 4530v2	1.4.3.1	2011 - 2018	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
EVS 6000 EVS 6010 EVS 6020 EVS 6030	1.5.0.0	2011 - 2018	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
EVS 6021 EVS 6030	1.5.1.0	2011 - 2018	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
EVS 6040 EVS 6043	1.5.2.0	2011 - 2018	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12

EVS 6040 AZ	1.5.2.1	2011 - 2019	e39d71e88398beb836ee95973be1daec2bdbc091619891d8026fbf a15ae1798e
EVS 6050 EVS 6051	1.5.3.0	2011 - 2019	e39d71e88398beb836ee95973be1daec2bdbc091619891d8026fbf a15ae1798e

Proposed Plan

We are asking ES&S to place all affected versions with the labs as a de minimus change. According to Section 3.4.2. of the EAC's Testing and Certification Manual, a de minimis change is defined as a change to a certified voting system's hardware, software, TDP, or data, the nature of which will not materially alter the system's reliability, functionality, capability, or operation. Under no circumstance shall a change be considered de minimis if it has reasonable and identifiable potential to impact the system's performance and compliance with the applicable voting Standard.

The bitmap file is "minor in nature and effect" and qualifies under section 3.4.1 for a change order.

The VSTLS will perform a thorough review of all source code in all affected versions and the EAC will receive reports on all versions.

The de minimus process will allow for election officials to have full assurance that the labs have thoroughly reviewed and compared all affected versions to the trusted build as part of the de minimus review.

We are requesting this effort be performed in an expedited manner and within a two week time frame. We will share our findings with you and keep you updated throughout the process.

In weighing the merits, we believe this is the most optimal solution given the non-substantive impact of the bitmap file issue that is causing the hash mismatch. This process will also allow for verification that the bitmap file is in fact the only change and will result in compliance with EAC's certification program.

This effort doesn't impact the state's/jurisdiction's ability to request ES&S to perform a clean full installation which would also resolve the hash value issue. Given the short time window left until the election, we wanted to implement a solution that resolves the issue for all while simultaneously allowing you to focus on all the hard work you are doing to run safe and secure elections.

Finally, this proposed plan is based on the information the EAC has right now. Should we learn new material information, we will modify the plan and take whatever steps are appropriate.

Sincerely,

Mona Harrington

Mona Harrington, Executive Director

cc:

Kevin Rayburn, General Counsel

Jerome Lovato Director, Voting System Testing and Certification

ELECTION SYSTEMS AND SOFTWARE (ES&S) CORRUPTION DOC

TABLE OF CONTENTS

Updated as of 7/16/2019, Previous Update 7/10/2019, New Bullets in Red

- **THEME 1: ES&S Pay-For-Play Schemes Run Rampant Across U.S. As Election Officials Trade Million Dollar Voter Machine Contracts for Donations and Gifts**
 - **Topic 1:** In Georgia—The Chief of Staff to the former Secretary of State, the Deputy Chief of Staff to the Governor, the head of Legislative Affairs for the former Governor, the former Secretary of State, and the former State Election Director—were all either ES&S lobbyists or accepted large donations/gifts from ES&S (PAGE 3)
 - **Topic 2:** In order to pass bill to purchase \$150 million of new, unsafe voting equipment (likely from ES&S), GA lawmakers repeatedly lied and produced data conservative groups deemed “profoundly misleading.” (PAGE 4)
 - **Topic 3:** On February 8, 2018, Georgia Secretary of State awarded ES&S with \$450,000 sole source contract—giving a private corporation direct access to and/or responsibility over voter registration, ballot access, and ballot counting until Dec 31st, 2019. (PAGE 8)
 - **Topic 4:** Massive conflicts of interest uncovered with ES&S and elections officials in New York, Arkansas, South Carolina, Pennsylvania, Texas, Louisiana, North Carolina, Ohio, and Florida (PAGE 12)
 - **Topic 5:** South Carolina republicans to reassess voter machine procurement after ES&S corruption uncovered during process to pick vendor for \$60 million contract (PAGE 16)
 - **Topic 6:** Pennsylvania state auditor warned of nationwide ES&S vendor corruption “If it’s happening here, it must be happening elsewhere.” (PAGE 18)
- **THEME 2: ES&S Lied to Federal Lawmakers Regarding Data Security and Consistently Demonstrated a Dangerous Lack of Competence in Creating Secure and Reliable Machines. Their “Criminally Negligent” Software Caused Election Altering Undervotes, Exposed the Personal Data of Millions, and Violated State Laws**
 - **Topic 1:** ES&S machines are directly tied to significant undervotes at every level in Georgia, Florida, Texas, Arizona, Pennsylvania, and North Carolina (PAGE 20)

- **Topic 2:** Ohio software called “highly dangerous,” “criminally negligent from the standpoint of data security” and “insanely risky” by election security experts. (PAGE 23)
- **Topic 3:** ES&S has consistently demonstrated a systematic disregard for basic security best practices and a complete lack of competence in the manufacturing of reliable voting machines (PAGE 25)
- **Topic 4:** ES&S large-scale negligence exposed personal data of millions of voters, left tens of thousands of names off rolls and led to massive delays in vote counts across the country (PAGE 25)
- **Topic 5:** US Senators express national security concerns after ES&S lied to federal lawmakers, refused to reveal which states were sent critically flawed machines, and vigorously fought attempts to reveal reliability information (PAGE 31)
- **Topic 6:** ES&S Indiana contract terminated after investigation reveals ES&S violated state law, lied to election officials, and were responsible for errors resulting in long wait times, voter anxiety, discouraged voters, and embarrassment. (PAGE 35)
- **Appendix:**
 - **A:** 2017 ES&S Security Test Report: Missing Operating Systems & Patches (PAGE 38)
 - **B:** Georgia Vendor RFI Analysis: Statewide Voting Machine Contracts (PAGE 39)
 - **C:** Map of Voting Systems Across the U.S.—Pew Research Center/Verified Voting Foundation (PAGE 40)

ES&S PAY-FOR-PLAY SCHEMES RUN RAMPANT ACROSS U.S. AS ELECTION OFFICIALS TRADE MILLION DOLLAR VOTER MACHINE CONTRACTS FOR DONATIONS AND GIFTS

IN GEORGIA—THE CHIEF OF STAFF TO THE FORMER SECRETARY OF STATE, THE DEPUTY CHIEF OF STAFF TO THE GOVERNOR, THE HEAD OF LEGISLATIVE AFFAIRS FOR THE FORMER GOVERNOR, THE FORMER SECRETARY OF STATE, AND THE FORMER STATE ELECTION DIRECTOR WERE ALL EITHER ES&S LOBBYISTS OR ACCEPTED LARGE DONATIONS/GIFTS

David Dove, Chief of Staff to former Secretary of State Brian Kemp, Accepted Las Vegas Trips From ES&S While His Office Was In The Market For New Voter Machines. In March of 2017, when Dove attended an E.S. & S. junket in Las Vegas, Kemp's office was in the market to replace the state's entire inventory of voting machines. "It's highly inappropriate for any election official to be accepting anything of value from a primary contractor," Virginia Canter, the chief ethics officer at Citizens for Responsibility and Ethics in Washington, told McClatchy. "It shocks the conscience." ([The New Yorker](#), 1/22/2019)

Kathy Rogers, Georgia's Former State Elections Director Who Opposed Paper Ballot Records, Is Now an ES&S Lobbyist and ES&S's Senior Vice President for Government Affairs. "Kathy Rogers, E.S. & S.'s senior vice-president for governmental affairs, told McClatchy that there was nothing untoward about the advisory board, which she said has been "immensely valuable in providing customer feedback."...In 2006, a bill requiring a verifiable paper record of each ballot, introduced in the Georgia legislature at the urging of election-integrity advocates, failed after the state's elections director, Kathy Rogers, opposed it. Rogers, of course, later went to work for E.S. & S. Election-integrity advocates sued in response, challenging the legality of the state's voting equipment." ([The New Yorker](#), 1/22/2019)

Karen Handel, Georgia's former Secretary of State, Received \$25,000 in Contributions From Voting Machine Lobbying Firm. "In the three years that the case wended its way through the courts, where it was eventually dismissed by the Georgia Supreme Court, the new secretary of state, Karen Handel, was found to have received twenty-five thousand dollars in campaign contributions from employees and family members associated with Massey and Bowers' lobbying firm." ([The New Yorker](#), 1/22/2019)

Charles Harper, Brian Kemp's current Deputy Chief of Staff and former Legislative Director, Was a Lobbyist for ES&S as Recently as June 2018. "In 2012, Charles Harper, a sod farmer who had been elected to the Georgia House of Representative a decade earlier, became a registered lobbyist in the office of the Georgia secretary of state, Brian Kemp, where he served as legislative director. At the end of 2017, as Kemp was ramping up his campaign for governor, Harper did not renew his lobbying credentials with the secretary of state. Instead, he registered to lobby for E.S. & S...After Kemp won the governor's race, in November, he named Harper, whose contract with E.S. & S. ended in June, 2018, to his transition team. Harper is now Kemp's deputy chief of staff." ([The New Yorker](#), 1/22/2019)

John Bozeman, the Head of Legislative Affairs for Former Governor Sonny Perdue, Has Been a Registered Lobbyist with ES&S Since 2017. “At the end of 2017, as Kemp was ramping up his campaign for governor, Harper did not renew his lobbying credentials with the secretary of state. Instead, he registered to lobby for E.S. & S. Around the same time, John Bozeman, then the head of legislative affairs for Georgia’s former governor, Sonny Perdue (who is now the Secretary of Agriculture in the Trump Administration), also registered to lobby on behalf of E.S. & S.” ([The New Yorker](#), 1/22/2019)

IN ORDER TO PASS BILL TO PURCHASE \$150 MILLION OF NEW, UNSAFE VOTING EQUIPMENT (LIKELY FROM ES&S), GA LAWMAKERS REPEATEDLY LIED AND PRODUCED ANALYSIS CONSERVATIVE GROUPS DEEMED “PROFOUNDLY MISLEADING”

Georgia Lawmakers Chose New Voting Equipment that Shared “Similar Risks” to Machines a Federal Judge Deemed a Constitutional Risk. “The new equipment would replace the state’s paperless, electronic machines — technology so risky that a federal judge said last year that its continued use threatened Georgians’ “constitutional interests.” But security researchers say similar risks exist in the new electronic machines that the GOP-led legislature has chosen, which would embed the voter’s choice in a barcode on a slip of paper.” ([Politico](#), 3/28/2019)

Cybersecurity Experts Said Georgia Lawmakers Made “False and Misleading” Statements that Flatly Contradicted Objective Evidence in Support of Bad Voting Machine Bill. “The bill’s sponsors made false and misleading statements during the entire legislative session in hearings leading up to the vote, often flatly contradicting objective evidence or mischaracterizing scientific writing,” said Georgia Institute of Technology computer science professor Rich DeMillo, who testified throughout the process.” ([Politico](#), 3/28/2019)

Two Conservative Groups Called GOP Sec. of State’s Brad Raffensperger’s Hand-Marked Ballot vs Machine Marked Analysis “Profoundly Misleading.” “Two conservative groups, the National Election Defense Coalition and FreedomWorks, called the voting-machine deal a “boondoggle” in a letter last week to state Senate Republicans. “The Secretary of State is circulating a cost analysis that is profoundly misleading and wildly inflates the costs of conducting elections with hand-marked paper ballots,” they wrote.” ([The New Republic](#), 3/06/2019)

GOP State Senator William Ligon Repeatedly Demonstrated a Lack of Understanding of Cyber Security and Ignored Warnings from Experts During Debate. “Ligon, who praised ballot-marking devices as “the technology of today built upon the experience of the past,” repeatedly demonstrated what experts called a lack of understanding about the cybersecurity implications of using computers to generate ballots, based on his comments during the Senate debate on the bill. “If there is any discrepancy discovered in an audit between what the machine says and what the paper says,” he assured his colleagues, “the paper will control.” But the paper ballot is generated by the machine and can thus be corrupted at the source, rendering a meaningful audit impossible. Stark, who invented the widely recommended audit technique known as a risk-limiting audit, warned Georgia lawmakers about this, but “they ignored his warning,” DeMillo said.” ([Politico](#), 3/28/2019)

State Sen. Ligon Falsely Stated that Barcode Devices and Hand-Marked Paper Ballots Posed Equal Hacking Risk. “State Sen. William Ligon, the bill’s chief defender in the chamber, said the barcode devices and hand-marked paper ballots were equally at risk of hacking. That’s just not the case, researchers said. “Hacking and configuration errors cannot cause pens to put the wrong votes on hand-marked paper ballots, but they can cause ballot-marking devices to print the wrong votes on the paper record,” Philip Stark, a statistics professor and voting security expert at the University of California at Berkeley, said in an email.” ([Politico](#), 3/28/2019)

State Sen. Ligon Falsely Stated that Optical Scanners Had Not Changed in 20 Years. “Ligon said the technology of optical scanners was “pretty much the same” as it was in 2000, even though, as DeMillo noted, “imaging capabilities have increased by orders of magnitude in the last twenty years.” ([Politico](#), 3/28/2019)

State Sen. Ligon Falsely Denied that Hand-Marked Paper Ballots Eliminated Need for Voter Verification. “During a colloquy with Parent, Ligon also denied (wrongly, experts said) that removing the ballot-generating computer — as hand-marked ballots do — eliminated the need for a voter to verify his or her ballot, despite this being one of the chief advantages of not using computers to mark ballots. (Research shows that voters using ballot-marking devices do not check to make sure the computer marked their ballot properly.)” ([Politico](#), 3/28/2019)

HB316 Bill Sponsor, Georgia State. Sen. Ligon, Later Claimed He Was Not Familiar with Recommendations Provided by Election Experts on the GA [SAFE] Commission. “Georgia state Senator William T. Ligon Jr. doesn’t agree that touchscreens are a less reliable method for casting votes. He was a sponsor of the bill, now signed into law, overhauling Georgia’s election system... Ligon said he wasn’t familiar with Lee and his advice to the commission.” ([Quartz](#), 7/9/2019)

GOP State Senator Greg Dolezal Falsely Stated that “Hackability” of Various Voting System Was Uniform. “Republican Sen. Greg Dolezal, too, said the “hackability” of various voting systems was “uniform,” despite the widespread consensus from technical experts that it’s not.” ([Politico](#), 3/28/2019)

GOP State Senator P.K. Martin IV Claimed, Without Evidence, that There Were No Instances of Hackers Breaching GA Voting Systems. “Sen. P.K. Martin IV, another Republican, said there had been “zero” instances of hackers breaching Georgia’s current voting machines. But there’s no evidence that hackers haven’t tampered with Georgia’s current voting system — paperless machines can be hacked to prevent any signs of tampering — and the machines have previously generated results that prompted questions about their reliability.” ([Politico](#), 3/28/2019)

Despite the National Academies Recommending Against Barcode Technology in Voting Systems Last Year, GOP State Rep Barry Fleming Claimed the Technology Would Bring GA Into the 21st Century. “Republicans largely hailed the [barcode] technology. “We can put our voters first in Georgia and bring us into the 21st century,” Republican state Rep. Barry Fleming said after the vote, according to The Atlanta Journal-Constitution... In a landmark report published last year, the National Academies recommended against voting devices that tally barcodes. “Electronic voting systems that do not produce a human-readable paper ballot of record raise security and verifiability concerns,” it said. “Additional research on ballots produced by BMDs will be necessary to understand the effectiveness of such ballots.” ([Politico](#), 3/01/2019)

GA State Senator, Elena Parent, Said the Relationship Between ES&S and GA Officials “Reeks of Corruption” and There is “No Good Reason” to Buy ES&S Machines. “Democratic state Sen. Elena Parent, who opposes the type of equipment the state is preparing to purchase — which includes an electronic marking device that produces a paper ballot — condemned the close ties between the company [ES&S] and the state. “I’ve been given absolutely no good reason why we should buy these things. There’s not one good reason. So therefore it just reeks of corruption, that we’re prioritizing vendors over voters,” Parent said on the Senate floor during a debate in March.” ([NPR](#), 5/2/2019)

ES&S Repeatedly Told Georgia State Officials That Its Machines Were Not Connected to the Internet, Despite Strong Disagreement from Cyber Security Experts. Quotes from ES&S Request For Information Response: “Furthermore, the EMS [Election Management System] system is closed (air-gapped) and therefore has no connection to the internet.” (pg. 17) “Standalone hardened system that is not connected to the Internet or any other network.” (pg. 17) “The data is accessed by the database server through a service account, thereby protecting the data files from being directly accessed. The EMS is isolated from any connection to the internet or other networks.” (pg. 18) ([ES&S GA RFI](#), 8/24/2018)

National Election Defense Coalition Said the Assertion Voting Machines Are “Not Connected to the Internet” is a Damaging Myth Preventing Election Officials from Using Paper Ballots. “The incorrect assertion that voting machines or voting systems can’t be hacked by remote attackers because they are ‘not connected to the internet’ is not just wrong, it’s damaging,” says Susan Greenhalgh, a spokeswoman for the National Election Defense Coalition, an elections integrity group. “This oft-repeated myth instills a false sense of security that is inhibiting officials and lawmakers from urgently requiring that all voting systems use paper ballots and that all elections be robustly audited.” ([NYT](#), 2/21/2018)

Cybersecurity Experts Explain Election Data Transmitted Via Phone Lines Are Still Connected to the Internet. “Election officials and vendors insist that the modem transmissions are safe because the connections go over phone lines and not the internet. But as security experts point out, many of the modems are cellular... These routers are technically part of the internet.” ([NYT](#), 2/21/2018)

Cybersecurity Experts Detail How Election Results Can Still Be Intercepted Since Phone Lines Are Part of the Internet. “Because of this, attackers could theoretically intercept unofficial results as they’re transmitted on election night — or, worse, use the modem connections to reach back into election machines at either end and install malware or alter election software and official results. “Almost any phone call, whether on a cellular network or a so-called landline, goes through a part of the internet,” says Andrew Appel, a computer-science professor at Princeton University and longtime voting-machine security expert.” ([NYT](#), 2/21/2018)

Georgia's SAFE Commission Ignored Security Measures Directly Recommended by Georgia Tech, Stanford, Yale, Princeton, MIT & Google Election Experts. "Earlier this year, Georgia's [SAFE] Commission held a public meeting at the state capitol to answer a pressing question: What should Georgia do to replace its aging, touchscreen voting machines, as well as other parts of its election system?... Computer scientists and elections experts from around the country had weighed in during the seven months of the commission's deliberations on the issue...Despite this, the commission ultimately did not recommend measures backed by Lee and his colleagues at places like Stanford, Yale, Princeton, MIT, and Google—including the recommendation that the state return to a system of paper ballots filled out by hand, combined with what scientists call risk-limiting audits." ([Quartz](#), 7/9/2019)

Elections Experts Fear Georgia's Ignorance of Election Security Issues Will be Copied by Other States & Cause Nationwide Erosion of Election Integrity. "Georgia's decision has computer scientists and election experts worried that lessons learned over nearly two decades of computerized voting are being woefully ignored. Indeed, hundreds of millions of dollars have been or will soon be spent in these and other states on technology that experts say decreases election security and erodes election integrity." ([Quartz](#), 7/9/2019)

Including Georgia, Only 33% of Counties Nationwide Use Machines with No Paper Trail or Machines that "Print" Ballots. "With its decision, Georgia's counties remain among the 33% of counties nationwide that use either machines with no paper trail or machines that print paper ballots, which are then scanned on separate machines. The vast majority of the rest of the counties use paper ballots filled out by hand, which are then scanned or counted by hand." ([Quartz](#), 7/9/2019)

Georgia New Machines May Run On Unsupported Software. "The AP surveyed all 50 states, the District of Columbia and territories, and found multiple battleground states affected by the end of Windows 7 support, including Pennsylvania, Wisconsin, Florida, Iowa, Indiana, Arizona and North Carolina. Also affected are Michigan, which recently acquired a new system, and Georgia, which will announce its new system soon. ([AP](#), 7/13/2019)

It Is Unclear Whether Georgia Counties Will Be Forced to Pay for Windows 10 Software Update. "Critics say the situation is an example of what happens when private companies ultimately determine the security level of election systems with a lack of federal requirements or oversight. Vendors say they have been making consistent improvements in election systems. And many state officials say they are wary of federal involvement in state and local elections. It's unclear whether the often hefty expense of security updates would be paid by vendors operating on razor-thin profit margins or cash-strapped jurisdictions." ([AP](#), 7/13/2019)

ES&S Implied "Jurisdictions" May Ultimately be Responsible for Updating Software Expenses. "ES&S said it expects by the fall to be able to offer customers an election system running on Microsoft's current operating system, Windows 10. It's now being tested by a federally accredited lab. For jurisdictions that have already purchased systems running on Windows 7, ES&S said it will be working with Microsoft to provide support until jurisdictions can update. Windows 10 came out in 2015. ([AP](#), 7/13/2019)

GA Sec of State Failed to Follow Federal Judge Orders to Preserve FBI Election Data Evidence After Secretly Deleting Data on State Server. “Nearly two years ago, state lawyers in a closely watched election integrity lawsuit told the judge they intended to subpoena the FBI for the forensic image, or digital snapshot, the agency made of a crucial server before state election officials quietly wiped it clean. Election watchdogs want to examine the data to see if there might have been tampering, given that the server was left exposed by a gaping security hole for more than half a year. A new email obtained by The Associated Press says state officials never did issue the subpoena, even though the judge had ordered that evidence be preserved, including from the FBI.” ([AP](#), 7/3/2019)

Brian Kemp Denied Ordering Election Data Destruction in 2017, Called Destruction “Reckless, Inexcusable, and Inept.” Technicians at the Center for Elections Systems at Kennesaw State University, which then ran the state’s election system, erased the server’s data on July 7, 2017, less than a week after the voting integrity suit was filed. After the AP reported on it three months later, Kemp denied ordering the data destruction or knowing about it in advance and called it reckless, inexcusable and inept. ([AP](#), 7/3/2019)

Georgia Officials Failed to Disclose that the Department of Homeland Security Warned them that the State May Be a Cyber Target. “As lawyers for Georgia’s secretary of state argued vehemently last fall that the state’s obsolete electronic voting infrastructure was secure from hackers, they failed to mention a warning from the U.S. Department of Homeland Security that Georgia might already be a cyber target. “Foreign governments may engage in cyber operations targeting the election infrastructure and political organizations in Georgia and engage in influence operations that aim to interfere with the 2018 U.S. elections,” according to a memo by the U.S. Department of Homeland Security Southeast region addressing “a Georgia Perspective on Threats to the 2018 U.S. Elections.” ([Law.com](#), 7/15/2019)

The Department of Homeland Security Warned Georgia Election Officials That Foreign Actors May Attempt to Enter Polling Places, Hack Voter Registration Systems, and Access Information Technology. “The DHS memo warned Georgia election officials that the agency’s Office of Intelligence and Analysis was particularly concerned that foreign actors would employ at least 10 different methods in efforts to interfere with the 2018 election in Georgia. They included: Unauthorized entry to polling places...Attempts to hack voter registration systems...Attempts to access information technology infrastructure used to manage elections, display results, or for counting or certifying votes...Efforts to compromise networks or election-related systems...” ([Law.com](#), 7/15/2019)

IN FEBURARY 2018, GEORGIA SECRETARY OF STATE AWARED ES&S WITH \$450,000 SOLE SOURCE CONTRACT – GIVING PRIVATE CORPORATION DIRECT ACCESS TO AND/OR RESPONSIBILITY OVER VOTER REGISTRATION, BALLOT ACCESS, AND BALLOT COUNTING THROUGH DECEMBER 31, 2019

In 2019 RFP, GASOS Said Their Office Was Responsible for Maintaining Voter Registration System, Building Ballots, and Creating Poll Book Files. “Election Structure: State law provides for a uniform voting system where every county uses the same type of voting equipment...The GASOS

maintains the Voter Registration System (“eNet”), builds ballots for each federal, state, and county election, and creates Electronic Poll Book (“EPoll”) files. ([GASOS RFP](#), 3/15/19)

In 2018, GASOS Transferred Georgia Election Data Preparation Services—Previously Performed by State Entity, Center for Election Systems—to Private Corporation, ES&S.

“Exclusive Capability: ...Assistance in data preparation requires a license to utilize both pieces of software. These services were previously provided by the Center for Election System, which, as a state entity, was able to utilize the license purchased by the State of Georgia from ES&S...Now that the functions of the Center for Election Systems have been moved to the State Entity, State Entity requires a vendor who has licenses to both components of the voting system to assist in the data preparation. State Entity also requires a vendor...who knows the specific processes utilized by the Center for Election Systems in how they built their data sets.” ([CGG Subpoena](#), page 15, 7/5/2019)

In 2018, GASOS Paid Private Corporation-ES&S \$300,000 to Prepare Data Necessary for the Entire Georgia Election Management System (GEMS) & for All Voter Rolls.

“Scope of Work: State Entity seeks to enter into a contract to provide assistance in data preparation for ExpressPoll 4000 and 5000 running EZRoster version 2.1.2 and the Georgia Election Management System (GEMS) database version 1.18.22g!... The cost will be \$25,000 per month for the calendar year 2018.” ([CGG Subpoena](#), page 14, 7/5/2019)

In 2019, GASOS Paid Private Corporation, ES&S, an Additional \$150,000 to Extend Data Preparation and Ballot Layout Services Through December 31, 2019.

“The Agreement between Election Systems & Software (“Contractor” or “ES&S”) and Georgia Secretary of State dated February 8, 2018 for Ballot Building Support Services is hereby renewed for a term of January 1, 2019 through December 31, 2019 and amended as set forth below:...Payment Terms: 50% of total due (\$75,000) shall be payable on January 1, 2019 upon receipt of corresponding contractor invoice. The remaining 50% of total due (\$75,000) shall be payable on July 1, 2019 upon receive (sic) of corresponding contractor invoice.” ([CGG Subpoena](#), page 12, 7/5/2019)

ES&S Prepared Election Data for All 159 Georgia Counties & for Every County, State, and Federal Race in 2018.

“State Entity requires data preparation for 159 counties for all county, state, and federal races in Georgia including primary, primary runoffs, general election, general election runoffs, and any special elections. The cost will be \$25,000 per month for the calendar year 2018.” ([CGG Subpoena](#), page 14, 7/5/2019)

GASOS Failed to Document Any Effort to Locate Other Vendors—Claimed Vendor Change Would Be “Too Costly.”

“Market Research: Sole Source: A purchasing situation in which the procurement is available from only one source. The announcement must be posted to the GPR in accordance with the Georgia Procurement Manual, Section 2.3.3.3. Question: Identify efforts made to locate other possible sources: Answer: “Current License provider for Georgia Election Management System. Changing systems would be to (sic) costly.” ([CGG Subpoena](#), page 19, 7/5/2019)

GASOS Claimed 2018 “Sole-Source” Award to Private Corporation, ES&S, Justified Because ES&S Was Only Company with Licenses to Work Both Components of Georgia’s Voting System.

“Sole-Source Intent to Award Justification: Exclusive Capability: The State of Georgia utilizes ExpressPoll 4000 & 5000 running EZRoster version 2.1.2 and GEMS version 1.18.22g!. Assistance in data preparation requires a license to utilize both pieces of software....ES&S provided both systems to the state and has a license to maintain both databases... ES&S has specific knowledge that is necessary to the fulfillment of these services and is the only company that has licenses to work with both components of Georgia’s voting system.” ([CGG Subpoena](#), page 15, 7/5/2019)

Election Expert Disputed GASOS Sole-Source Argument Claim—Said GASOS Awards Licenses, Not the Vendor/ES&S. “Vendors are in the business of providing software licenses for a fee, so election administrators should be the ones to get a license to use the necessary software. In the U.S., our federalist system says that election officials administer elections –not private corporations. ([Twitter](#), @eddiepereztx, 7/5/2019)

Election Expert Said GASOS Claim that Only ES&S Could Provide Election Administration Services “Exceptional” and Uncommon. “NOT common (exceptional): D) Assertions by a state or county authority that no one other than the vendor can provide election administration services, because no one other than the vendor has a license to use voting system software.” ([Twitter](#), @eddiepereztx, 7/5/2019)

Election Expert Said Georgia Sec. of State’s Decision to Pay ES&S to Maintain Election Databases Was “Atypical” & “NOT common.” “NOT common (atypical): C) Paying a vendor to *maintain* ballot programming databases. (Once the vendor’s ballot programming is complete, the databases are typically turned over to state or county election officials, so they can run the election under their own auspices).” ([Twitter](#), @eddiepereztx, 7/5/2019)

Election Expert Said Georgia’s 2018 Contract with ES&S “Robbed” State & County Officials Power to Run their Own Elections. Vendors are in the business of providing software licenses for a fee, so election administrators should be the ones to get a license to use the necessary software. In the U.S., our federalist system says that election officials administer elections — not private corporations. 6/ Saying “Only the vendor that holds the license has the license to use election software” is tautological, and it robs both the state and county officials from having the wherewithal to run their own elections.” ([Twitter](#), @eddiepereztx, 7/5/2019)

Contract Said ES&S is Responsible for All Ballot Layout, Coding & Voice File Services in Georgia. “1. BALLOT LAYOUT, CODING, AND VOICE FILE SERVICES – Scope of Services includes the data entry and maintenance of County level databases in the State of Georgia for all county (including municipal elections that are administered by counties), state and federal elections in Georgia in calendar year 2019, including primary, primary runoffs, general election, general election runoffs, and special elections. ES&S will receive the data required to facilitate the creation of paper and electronic ballots as well as audio file recording to the State of Georgia for review and approval.” ([CGG Subpoena](#), page 12, 7/5/2019)

Election Expert Said Counting of Votes Should “Never, Ever” be Done by the Vendor. “If a state or local official outsources programming, that’s one thing; but the actual tabulation function, i.e. insertion of memory cards into the tabulation computer, and the counting of the votes, should be done solely by election officials, and never, ever by the vendor.” ([Twitter](#), 7/5/2019)

Texas Secretary of State’s Office Said ES&S Ballots Failed to Present Candidates Consistently or Separate Races Properly During Initial Examination. “The full-face ballot layout used during the examination was less than ideal. Too much of the available screen real estate was unused. Also, the candidates were not presented consistently for each race. Sometimes the candidates for a race were presented vertically and sometimes they were presented horizontally.” ([Texas Secretary of State](#), 1/22/19)

Texas Secretary of State’s Office Said ES&S Poor Ballots Designed Caused Candidates to be “Lost in the Mix” During Initial Examination. “Ballot layout requires consideration of how the candidates and parties are displayed. At the very least, a blank line or race separator (i.e. double line) should be between each race. This should be enforced by the layout software so the ballot isn’t presented like the test ballot which had races stacked on top of each other. With many candidates listed across the columns, and no gap before the next race, some of the candidates were “lost” in the mix due to their unfavorable location. The ES&S representative said that the poor layout was because she is not an expert in ballot design on the XL.” ([Texas Secretary of State](#), 1/22/19)

ES&S Representative Failed to Properly Display Candidates During State Examination—Said She was “Not an Expert in Ballot Design.” “With many candidates listed across the columns, and no gap before the next race, some of the candidates were “lost” in the mix due to their unfavorable location. The ES&S representative said that the poor layout was because she is not an expert in ballot design on the XL.” ([Texas Secretary of State](#), 1/22/19)

ES&S is Responsible for All Data Entry & Maintenance of County Level Data Sets in Georgia. “2. EXPRESSPOLL DATA SETS FOR ADVANCE VOTING PURPOSES – Scope of Services includes the data entry and maintenance of County level data sets in the State of Georgia for all county (including municipal elections that are administered by counties), state, and federal elections in Georgia in calendar year 2019, including primary, primary runoffs, general election, general election runoffs, and special elections. ES&S will receive the data required to facilitate the creation of ExpressPoll data sets for Advance Voting purposes to the State of Georgia for review and approval. Creation of ExpressPoll data sets does not include any handling or conversion of voter data.” ([CGG Subpoena](#), page 12, 7/5/2019)

ES&S Provided Georgia with its Election Management System & Has License to Maintain that System. Purpose of the Sole Source. The State of Georgia utilizes ExpressPoll 4000 & 5000 running EZRoster version 2.1.2 and GEMS version 1.18.22g!...ES&S provided both systems to the state and has a license to maintain both databases. Through contracts with all Georgia counties, ES&S has been the sole maintenance provider on the system since its purchase... ([CGG Subpoena](#), page 18, 7/5/2019)

GASOS Stated EPoll Data Management System (EPDMS) Combines Voter Registration & Election Ballot Data into Voter Lists for Poll Books & Voter Specific Ballots. “EPoll Data Management System (EPDMS) – Used to combine voter registration and election ballot data into an election-specific elector’s list that powers the electronic poll book (EPoll) and provides each voter with the properly assigned ballot style.” ([GASOS RFP](#), Attachment M, 3/15/19)

GASOS Stated EPDMS Must Accept Imports of Voter Registration Data from eNet Including Voter Name, Driver License Number, Voter Status, & Voter Polling Place.

“Confirm That Capability Exists and is Able to be Demonstrated: Capabilities: a. Accept imports of voter registration data from eNet on removable devices for the purposes of building an elector’s list for any given election. The data transferred from eNet includes but is not limited to: Voter Name...Voter Street Address, Voter City, State, Zip, Driver License number, Voter Registration ID, Voter Status, Assigned Precinct, Assigned District Combination Value, Assigned Polling Place, Polling Place Street Address, Polling Place City, State, Zip, and Absentee Status. ([GASOS RFP](#), Attachment M, 3/15/19)

Winning Vendor of RFP Process Must Complete Pilot Program In 10 Counties During November 2019 Election. “For the purposes of this eRFP, the Supplier’s preliminary plan and estimates for delivery are to be in a phased roll-out as a pilot project and then a full roll-out to all counties. Phase 1 will be the full inventory distribution and necessary training of up to 10 counties selected by GASOS to participate in a pilot project to be executed in November 2019. The pilot equipment will be used in any associated November 2019 election schedule for the selected counties.” ([GASOS RFP](#), Page 42, 3/15/19)

Winning Vendor of RFP Process Must Distribute 1,272 Voting Machine Components by December 31, 2019. “Phase 2 will be broken into two parts. Phase 2-Part 1 will be distributing a minimum of five BMD, two PPS, and 1 EMS computer to each county (159). These components will facilitate election official and poll worker training activities...Completion of Phase 2 – Part 1 will be completed by endo for the fourth quarter of 2019 (December 31st 2019).” ([GASOS RFP](#), Page 42, 3/15/19)

GASOS Said ES&S “Knows the Specific Processes” Used by KSU’s Center for Election Systems to Build Their Data Sets. “ES&S also worked closely with the Center for Election Systems and is most familiar with the processes it utilized to provide these data sets...State Entity also requires a vendor who best knows the Georgia voting system, who is familiar with Georgia counties, and who knows the specific processes utilized by the Center for Election Systems in how they built their data sets.” ([CGG Subpoena](#), page 15, 7/5/2019)

MASSIVE CONFLICTS OF INTEREST UNCOVERED WITH ES&S AND ELECTIONS OFFICIALS IN NEW YORK, ARKANSAS, SOUTH CAROLINA, PENNSYLVANIA, TEXAS, LOUISIANA, NORTH CAROLINA, OHIO AND FLORIDA

In Order to Secure \$40 Million NY Contract, ES&S Paid Anthony Mangone \$50,000 to Act as Lobbyist--Despite Mangone Being Under Federal Investigation for Corruption and Previously Pleading Guilty to Election Rigging (2010). "While a Republican lawyer was under federal investigation in a Yonkers corruption case, he was paid nearly \$50,000 last year to help a Nebraska company win a contract to provide New York City with new voting machines. Anthony Mangone was indicted this month with Yonkers Councilwoman Sandy Annabi and former city GOP Chairman Zehy Jereis on extortion, bribery and other federal charges related to payments made to Annabi for her to change votes on city projects. Coincidentally that same day, the New York City Board of Elections voted to buy thousands of new electronic voting machines - a contract expected to be worth more than \$40 million - from Mangone's client, Election Systems & Software...Mangone was implicated in a Westchester vote-rigging scheme a decade ago, admitting that he opened about 30 sealed absentee ballots during the 2000 Green Party primary and wrote in the names of his boss, Republican state Sen. Nicholas Spano, and a judicial candidate... Mangone agreed to plead guilty to a misdemeanor in the case but was never charged." (*The Journal News*, Bandler, 1/21/2010)

New York Board of Elections Head Resigned From ES&S Advisory Board After Conflicts of Interest Uncovered (2018). "The head of the city's Board of Elections Michael Ryan, a native Staten Islander, abruptly resigned from his post on the advisory board of the maker of New York City's voting machines, Election Systems and Software (ES&S), earlier this week. His resignation came after a NY1 report found that ES&S had flown Ryan around the country to destinations like Las Vegas putting him up in hotels and buying him dinners. Ryan reportedly did not disclose several ES&S paid trips in his annual disclosure forms with the city's conflict of interest board." ([SI Live](#), 10/13/2018)

Arkansas Secretary of State Bill McCuen Pleaded Guilty to Felony Charges that He Took Bribes and Accepted Kickbacks from Company that Would Become ES&S (2002). "Arkansas. February 2002. Arkansas Secretary of State Bill McCuen pleaded guilty to felony charges that he took bribes, evaded taxes, and accepted kickbacks. Part of the case involved Business Records Corp. now merged into Election Systems & Software. The scheme also involved Tom Eschberger, an employee of BRC, but Eschberger received immunity from prosecution for his cooperation. Today, Eschberger remains employed with ES&S." ([Voters Unite](#), 7/10/2007)

South Carolina's Director of Elections Resigned From ES&S Advisory Board Right Before State Reviewed Voting Machine Bids, Claimed No Impropriety After Conflicts of Interest Uncovered. "For more than a decade, Marci Andino, executive director of the S.C. Election Commission, served on an advisory board formed by Elections Systems and Software, known commonly as ES&S. Andino received more than \$19,000 worth of flights, hotels and meals from ES&S since 2009 to attend regular conferences at the company's headquarters in Nebraska and other cities across the country, according to records with the South Carolina Ethics Commission...On Monday, Andino confirmed she stepped down from her advisory position with the company last year in anticipation of the state requesting bids for a new voting system. She promised her connection to ES&S would in no way impact the state's decision over which company wins the multimillion dollar contract. Andino said she will not be taking part in selecting the winning bid." ([Post & Courier](#), 1/29/2019)

Pennsylvania County Election Director Resigned From ES&S Advisory Board Right Before County Vote To Purchase ES&S Poll Book System, Claimed No Impropriety After Undisclosed Conflicts of Interest Uncovered. “Crispell traveled to Las Vegas and Nebraska last year for meetings of the Election Systems & Software (ES&S) customer advisory board. Her travel expenses were paid for by ES&S, which supplied the voting machines Luzerne County has used for more than 10 years, as well as an electronic poll book system the county purchased this year for \$324,802. Crispell resigned from the advisory board in October 2017, before the county requested proposals for the poll book system from vendors. She did not disclose her service on the board to county council before it voted on the poll book purchase, in April.” ([Citizens' Voice](#), 12/7/2018)

Dallas, Texas Elections Administrator Asked To Resign After “Troubling” ES&S Conflicts of Interest Uncovered. “State ethics laws are clear when it comes to the relationship between public officials and vendors. Over the past two years, Dallas County has paid them or their subsidiaries \$3.5 million dollars for software and services. As Dallas County Elections Administrator, Toni Pippins-Poole recommends to the Commissioners Court which vendors get hired...In a June 7 email, she asks a county employee... “Have you checked with [vendor] ES&S to sponsor the Texas Delegation pins for IGO or the shirts?” The next day, a representative from ES&S emailed Pippins-Poole regarding paying for the lapel pins. He writes... “In the past we simply wrote a check to Toni...” He adds...“We can send a check made out to you (Toni) for the \$1500 amount....”“For an elections administrator to solicit contributions from a vendor is troubling,” said Joe Kulhavy, a former staff attorney for the Texas Secretary of State’s elections division who looked at Pippins-Poole’s emails at WFAA’s request.” ([WFAA ABC](#), 10/19/2017)

“A candidate for Dallas County commissioner on Tuesday asked a judge to remove Elections Administrator Toni Pippins-Poole from office, alleging incompetence and official misconduct. J.J. Koch, a Republican, accused Pippins-Poole of improperly soliciting a gift from a county contractor.” ([Dallas News](#), 10/2017)

Louisiana Elections Commissioner Accepted \$3000 in Donations from ES&S Prior to Recommending ES&S for a \$4 Million Voting Machine Contract. “Elections Commissioner Suzanne Terrell won praise for the way she selected the vendor for computerized absentee voting machines. But Legislative Auditor Daniel Kyle said he was still troubled by the selection of a company that has a top official who was allegedly involved in illegal dealings in Arkansas...Terrell was given a chance to explain how she chose Elections Systems and Software for a \$4 million contract to provide the new voting machines...Terrell said she has contributed Eschberger's \$2,000 campaign gift to a charity, later identified by staff aide Pat Bergeron as Girls' State. She said it was "naive" of her to have accepted the gift from Eschberger and another \$1,000 contribution from the Adams and Reese law firm that lobbies for ES&S.” (*Daily Town Talk*, Morgan, 2/7/2002)

North Carolina Election Directors Accepted Large Cash Donations From ES&S, Allowed Vendors to Charge Double for Ballots, After \$3 Million Statewide Voting Machine Contract. “A group made up of election directors from across North Carolina has received large cash donations from the owner of a New Bern company that maintains the state's voting machines and prints most of its ballot...Printelect is the sole agent in the state for Election Systems & Software, a company that won a concession in 2006 to sell and maintain all of the voting machines in the state. That arrangement gives

Print elect, which also represents ES&S in South Carolina and Virginia, a big advantage in getting printing jobs. The company prints ballots for 85 of the North Carolina's 100 counties, sometimes charging double what it costs to buy from a competitor not certified by ES&S." (*The News & Observer*, Biesecker, 08/11/2010) (\$3 Million Contract [Link](#))

North Carolina Board of Elections Delayed Certification of ES&S Machines Until Security Concerns Regarding Company Ownership Disclosed. "The State Board of Elections said cybersecurity worries prompted a delay in certifying election system vendors to sell voting machines to counties. In her first state board meeting Thursday, June 13, new Executive Director Karen Brinson Bell urged the board to require vendors seeking certification to disclose all ownership interests of 5% or greater. After a lengthy closed executive session, the board unanimously approved Bell's proposal... The board was scheduled to certify three voting machine vendors — Massachusetts-based Clear Ballot, Nebraska-headquartered Election Systems & Software, and Hart Intercivic of Texas." (*The Daily Courier*, Way, 6/20/2019)

Deputy Director of Franklin County, Ohio Board of Elections Lied to Board, Failed to Disclose He Was Offered a Job By ES&S, and Failed His Wife was on Board of ES&S linked Group In order to Ensure \$12.3 Million ES&S Contract Signed. Conflict-of-interest questions surrounding Michael R. Hackett Jr.'s relationship with owners of SST Systems, a New Albany company that supplies storage carts for voting machines, concerned board members for much of last year. Those worries appeared to be resolved on Nov. 23, when elections board Director Matthew Damschroder, a co-worker and close friend of Hackett's, told the board, "We've consulted with the county prosecutor and there are no conflicts of interest." The board then approved the SST contract. But County Prosecutor Ron O'Brien said last week that he never cleared Hackett of conflict questions. (*The Columbus Dispatch*, 5/14/2006)

Ohio Election Official Joined Board of ES&S Linked Company Despite Ohio Ethics Board finding "Significant Issues" With the Arrangement. "In fact, when an Ohio Ethics Commission lawyer took an initial look at the relationship, she said there were "significant issues" with the arrangement. Hackett did not respond to the lawyer's questions for almost four months, and then he retired without receiving an opinion from the commission... For three or four months last year, Hackett's wife, Mary, was a one-third partner in SST. The company was incorporated in January 2005 by Mrs. Hackett; John Fike, one of Mr. Hackett's childhood friends; and Richard Prohl. On Jan. 3, five weeks after he retired from the board, Mr. Hackett became a partner of Fike and Prohl's by forming an affiliate of SST. * For months last year, SST Systems was negotiating a sales agreement with Election Systems & Software, a Nebraska-based company that was simultaneously seeking a contract to supply Franklin County's new voting machines." (*The Columbus Dispatch*, 5/14/2006)

Former Florida Secretary of State Profited by Acting as ES&S Lobbyist and as the Lobbyist for State Counties To Receive Vendor Recommendations. "A former Florida secretary of state profited by being a lobbyist for both the state's counties and the company that sold some of them touchscreen voting machines used in last month's botched primary election. Sandra Mortham, who served as the state's top elections official from 1995 to 1999, is a lobbyist for both Election Systems & Software and the Florida Association of Counties, which exclusively endorsed the company's touchscreen machines

in return for a commission...After the association's June 2001 endorsement, ES&S received orders totaling more than \$70.6 million from Florida counties. That includes Miami-Dade County's \$24.5 million purchase and Broward County's \$18 million contract. The association will receive about \$300,000 in commissions, according to the agreement." (*AP News*, 10/5/2002)

After John Bel Edwards was Elected Governor of Louisiana, He Sided With ES&S and Successfully Blocked a \$95 Million Voting Machine Contract Awarded to Their Competitor.

"Ardoin's office had announced Aug. 9 that it had selected Dominion to replace Louisiana's current stock of voting machines, which were last purchased in 2005...The \$95 million contract was held up a few weeks after it was awarded when one of the losing bidders, Election Systems & Software, the largest U.S. manufacturer of voting equipment, objected to the contracting process." ([State Scoop](#), 10/11/2018)

Between 2014-2018, ES&S Donated \$13,250 to Louisiana Governor John Bel Edwards (D).

"Louisiana campaign finance records show that ES&S's lobbyist in Baton Rouge, William "Bud" Courson, has donated \$13,250 to Edwards' campaigns since 2014." ([State Scoop](#), 10/11/2018)

"Independent" Voting Machine Testing Labs Accepted Thousands of Dollars in Donations From ES&S. "The private testing system of independent labs was created in 1994 by a group of election officials who were brought together by the National Association of State Election Directors (NASED)...In 2002, the Houston-based Election Center operated on a \$462,000 budget. Executive Director Doug Lewis said Election Center's budget comes mostly from membership dues and training fees. But he acknowledges accepting up to \$10,000 a year in donations from voting-equipment manufacturers like Sequoia Voting Systems and Election Systems & Software. That doesn't sit well with California's top election official. "Where I come from, any firm regulatory or approval scheme should be conducted by entities that are entirely independent from any reliance -- financial or otherwise -- from the people that they have to oversee," Shelley said." (*San Jose Mercury News*, Ackerman, 5/30/2004)

SOUTH CAROLINA REPUBLICANS TO REASSESS VOTER MACHINE PROCUREMENT AFTER ES&S CORRUPTION UNCOVERED DURING PROCESS TO PICK VENDOR FOR \$60 MILLION STATE CONTRACT

South Carolina's Election Commission Executive Director, Marci Andino, Proposed \$60M ES&S Contract After Serving on ES&S Advisory Board and Receiving Over \$19,000 Worth of Flights, Hotels Meals, and Conferences From ES&S. "The relationship between South Carolina's director of elections and the country's largest voting equipment company has caught the attention of lawmakers as the state prepares to spend a proposed \$60 million to replace 13,000 voting machines. For more than a decade, Marci Andino, executive director of the S.C. Election Commission, served on an advisory board formed by Elections Systems and Software, known commonly as ES&S. Andino received more than \$19,000 worth of flights, hotels and meals from ES&S since 2009 to attend regular conferences at the company's headquarters in Nebraska and other cities across the country, according to records with the South Carolina Ethics Commission." ([Post & Courier](#), 1/29/2019)

S.C. Republican Lawmaker Said Conduct by ED of Election Commission May Give the Appearance of a Conflict and Urged Director to Avoid All Involvement in Solicitation Process.

“Some of the lawmakers advocating for a new voting system in South Carolina worry Andino’s connection to ES&S could cause the public to question that relationship, especially if the company is awarded another state contract. “I think if we’re not careful it gives the appearance — and underline that, the ‘appearance’ — of a conflict,” Rep. Kirkman Finlay, R-Columbia, said. “The director should avoid any and all involvement in the solicitation of bids.” ([Post & Courier](#), 1/29/2019)

S.C. Republicans Called for More Oversight and Transparency In the Bidding Process for Voting Machines, Move to Reassess Procurement Process, After Conflict of Interests Arise.

“But lawmakers are working on a joint resolution to give the State Fiscal Accountability Authority — made up of top S.C. elected officials — the authority to approve or veto that decision. We feel like there needs to be some more oversight and the process needs to be a little bit more open,” said state Rep. Kirkman Finlay, a Columbia Republican on the House Ways and Means Committee. “A lot of vendors, a lot of individuals, a lot of groups have contacted us and felt it was moving a little too quickly. With something like voting machines, we need to make sure everybody is included and everybody gets a shot at it.” ([The State](#), 2/21/2019)

S.C. Chooses to Limit the Election Commission’s Authority to Buy New Voting Machines Amid Concerns Over the Commission Director’s Relationship with ES&S. “S.C. lawmakers are working to limit the State Election Commission’s authority to buy new voting machines, amid concerns over the projected cost and the commission director’s longtime relationship with a possible vendor [ES&S]. ([The State](#), 2/21/2019)

South Carolina Approves \$51Million Contract for ES&S Despite Long History of Pay-For-Play with Election Officials. “State officials on Monday announced that a \$51 million contract had been awarded to Election Systems and Software, the nation's largest voting equipment vendor, to provide the new voting machines which promise more security in producing a paper ballot...The company also has ties to elections officials in South Carolina and other states, an investigation by McClatchy and The State revealed...For at least nine years, ES&S invited dozens of state and local elections officials to serve on an "advisory board" that gathers twice annually for company-sponsored conferences, including at a ritzy Las Vegas resort hotel, a McClatchy investigation found. Andino was among the attendees. The State reported last June that the company had covered \$19,200 in expenses associated with those trips for Andino during her decade as an adviser for ES&S.” (*The State*, Barton, 6/10/2019)

South Carolina League of Women Voters Criticized Decision, Said Hand Marked Paper Ballots Cost Half as Much as ES&S Machines and Are More Secure. “Critics of the Election Commission, including the League, say the state could move toward hand-marked ballots that can't be hacked at half the projected cost -- about \$25 million. Teague contends poorly designed ES&S software has led to problems in the past, including miscounted votes, according to League audits of South Carolina elections. She also argued hand-marked ballots have worked well in other states, and problems reading them have been exaggerated. "We are paying extra money for something that produces extra problems," she said. (*The State*, Barton, 6/10/2019)

PENNSYLVANIA STATE AUDITOR WARNED OF NATIONWIDE ES&S VENDOR CORRUPTION “IF IT’S HAPPENING HERE, IT MUST BE HAPPENING ELSEWHERE.”

Pennsylvania State Auditor Warned Auditors Nationwide to Review Potential ES&S Corruption.

“Even if this activity was permitted under the law, county officials who are making decisions about spending taxpayer dollars should not accept anything of value from the companies that are asking for their business,” DePasquale said... Costs are expected to range from \$125 million to \$150 million...DePasquale is urging auditors general nationwide to conduct similar reviews of elections-related gifts. “If it’s happening here, it must be happening elsewhere,” he said. ([TribLive](#), 2/22/2019)

Pennsylvania State Auditor Called For Stronger Ethics Rules to Prevent County Officials From Benefiting from Voting Machine Vendor Corruption. “DePasquale called for updating disclosure laws and strengthening state ethics rules to encompass more public officials. He said it doesn’t matter if the gifts were large or small. He took issue with the fact that people accepted them. “Even if this activity was permitted under the law, county officials who are making decisions about spending taxpayer dollars should not accept anything of value from the companies that are asking for their business,” DePasquale said.” ([TribLive](#), 2/22/2019)

Pennsylvania State Auditor Cited Several Counties For Accepting Gifts From ES&S That “Smacks Of Impropriety.” Elections officials in Western Pennsylvania say they’re rethinking accepting even small gifts like coffee and doughnuts from potential vendors after state Auditor General Eugene DePasquale flagged counties around the state for behavior that “smacks of impropriety.” Westmoreland, Butler and Washington counties were among those cited for accepting gifts from voting machine vendors since 2016. ([TribLive](#), 2/22/2019)

Pennsylvania State Auditor Was Concerned When ES&S Offered Flights to Las Vegas, Tickets to Wine Festivals, Admission to Amusement Parks, Dinners at High End Restaurants, and Open Bars at Conferences to Public Officials in 27% of Pennsylvania Counties. “Flights to Las Vegas, tickets to wine festivals, admission to an amusement park, dinners at high-end restaurants and open bars at conferences were among gifts that companies provided to public officials in 18 of Pennsylvania’s 67 counties, DePasquale said in a report released Friday. “As Pennsylvania counties choose new voting equipment, I want them to make decisions based on the best interest of voters — and no other factors,” DePasquale said.” ([TribLive](#), 2/22/2019)

Philadelphia City Controller Refused to Approve Payment for ES&S Voting Machines Amid Process and Legal Concerns. “Philadelphia City Controller Rebecca Rhynhart says she will not approve payment for new voting machines that will cost the city tens of millions of dollars. “I’m deeply concerned about the legality of this process,” she said in a statement Tuesday night, “and as city controller, I will not release \$1 of payment while these questions go unanswered.” ([The Inquirer](#), 5/1/2019)

Philadelphia Controller is Investigating Accusations Voting Machine Selection Process Biased to Favor Electronic Voting Machines Over Paper Ballots. “Until her office completes an investigation of the voting-machine selection process, including accusations that it was biased to favor electronic voting machines over paper ones that voters fill out manually, Rhynhart said she won’t sign

off on payment. Her approval is one of several that are required along the way when the city purchases new equipment or services.” ([The Inquirer](#), 5/1/2019)

Philadelphia Commission Approved ES&S Machines Despite Fierce Criticism from Controller, Auditor General and Hand-Marked Paper Ballot Supporters. “The Philadelphia city commissioners chose a new voting machine system Wednesday to be used starting in November, despite criticism of the process from the city controller, the state auditor general, and a group of advocates who want hand-marked paper ballots.” ([The Inquirer](#), 2/20/19)

Unnamed City Employees Selected ES&S Through a “Fast-Track and Secret Selection Process.” “New voting machines were selected Feb. 20 by two of the three current commissioners, Lisa Deeley and Al Schmidt, after a fast-tracked and secret selection process in which a committee of unnamed city employees evaluated proposals from vendors and made recommendations to the commissioners. Deeley has defended that process as intentionally rushed to meet Gov. Tom Wolf’s directive to purchase new machines by next year and intentionally secretive to protect it from outside influence, in accordance with city rules.” ([The Inquirer](#), 5/1/2019)

Commissioner Anthony Clark Voted Against the Proposal Because He Was Denied All Information Pertaining to the Selection Process as it Occurred. “Later, he called The Inquirer to reiterate his position. He said that since he had not signed a confidentiality form that would have allowed him to receive information on the selection as it was occurring, he was essentially left out of the process. He added that he learned about the machines only at the public meetings and as advocates criticized the system. “I didn’t have enough information,” Clark said. “I didn’t even know what options were available, because I didn’t sign the confidentiality [form] and no information was coming to me.” ([The Inquirer](#), 4/10/19)

Pennsylvania Councilwoman Called For ES&S to be Removed from Consideration of \$4M Contract Following Pay-For-Play Controversy. “Luzerne County Councilwoman Linda McClosky Houck has called for a potential vendor of planned new voting machines to be removed from the process, based on the company’s ties to the county election director...The company, known as ES&S, became embroiled in controversy in December when it came to light that county election director Marisa Crispell had served on the ES&S advisory board in 2017, and attended advisory board meetings for which the company paid her travel expenses. The county plans to purchase new paper-trail voting machines this year, to comply with a directive from state officials. The new voting system will cost about \$4 million, county officials said. (*The Citizen’s Voice*, Mark, 6/19/2019)

Pennsylvania Officials Say “Almost Impossible” for Voting Machines to be in Place for November Elections Given Training Required. “McGinley said he hopes the committee will forward its recommendation to council this summer. However, it is not likely the new voting machines will be in place for the November election, as officials had hoped, according to county Manager David Pedri. Even if the machines arrive in time, the amount of training required for election officials, poll workers and voters would make that almost impossible, Pedri said.” (*The Citizen’s Voice*, Mark, 6/19/2019)

Pennsylvania Governor Announced \$90 Million Bond Issue to Fund State Mandated Voting Machines. “Pennsylvania Gov. Tom Wolf announced a \$90 million bond issue Tuesday to fund a statewide voting machine upgrade effort that he ordered more than a year ago to ensure that every

vote cast creates a paper trail that can be checked by voters and audited ... The statewide voting machine upgrade requires all counties to use new systems with paper trails that voters can verify in plain text before casting their votes, allowing for audits and manual recounts. While some counties have used paper-based systems for years, most Pennsylvania voters have used insecure systems that store votes electronically.” ([The Philadelphia Inquirer](#), 7/9/2019)

ES&S LIED TO FEDERAL LAWMAKERS REGARDING DATA SECURITY AND CONSISTENTLY DEMONSTRATED A DANGEROUS LACK OF COMPETENCE IN CREATING SECURE AND RELIABLE MACHINES. “CRIMINALLY NEGLIGENT” SOFTWARE CAUSED ELECTION ALTERING UNDERVOTES, EXPOSED PERSONAL DATA OF MILLIONS, AND VIOLATED STATE LAWS.

ES&S MACHINES ARE DIRECTLY TIED TO SIGNIFICANT UNDERVOTES AT EVERY LEVEL IN GEORGIA, FLORIDA, TEXAS, ARIZONA, PENNSYLVANIA, AND NORTH CAROLINA

Georgia’s ES&S Unreliable Machines Led to an Undervote In the Lieutenant Governor’s Race of over 60,000 votes (2018). “The conduct of the election “was so defective and marred by material irregularities as to place in doubt the result of the election under Georgia law. This court should therefore declare the contested election invalid and set the date for a second election between the same candidates,” the lawsuit states... “Citizens must not permit flawed elections to stand,” said Bruce Brown, an Atlanta-based attorney representing the plaintiffs... The lawsuit notes the lieutenant governor’s race reported only 3,780,034 votes, while every other statewide race tally exceeded 3.843 million votes. The plaintiffs allege that “this high under-vote rate is a likely result of the touchscreen voting system malfunctions, and that the un-auditable system does not permit a reliable determination of the vote count.” ([AP News](#), 11/24/2018) (Note: GA signed a [\\$54 million voting machines deal](#) with Diebold Election Systems in 2002, Diebold sold Election System [business to ES&S](#) after Antitrust lawsuit in 2009.)

In 2015, Georgia Officials Said State Protocol Required Every Precinct in Every County to Compare Tabulated Results with Physical Poll Tape to Avoid ES&S Software Bug that Causes Undervote. “Some counties in Virginia and Georgia still use the problem software, as well. But they employ special protocols to make sure that votes aren’t dropped, officials in both states say. In Georgia, that includes comparing tabulated precinct results with each physical poll tape—essentially replicating Smith’s experiment, but for every precinct in every county.” ([Bloomberg](#), 9/29/2016)

ES&S General Election Software “Dropped” Over 1000 Votes from Black Precincts in Memphis—Some Were Incorrectly Labeled “Double Votes” By the System. “Not all of the precincts are named in the e-mail, but a master record for the voting machines shows missing uploads at four polling places on election night, all in areas with large concentrations of black voters. Three are located at black churches... The weird thing is, the GEMS system recognized at least some of the missing votes—stored on the memory cards of seven voting machines—as already counted when officials tried to reload them on Oct. 19, according to an e-mail exchange between Young and operations manager Darral Brown. But it was clear from Smith’s poll tape and other data dug up by

Young that they hadn't been. In all, 1,001 votes had been dropped from the election night count, according to the master record, including almost 400 from an early voting center at Mt. Zion, the most from any single polling place." ([Bloomberg](#), 9/29/2016)

2015 Memphis Undervote Caused by Software Bug ES&S [Diebold] Aware of Since 2008. "Among the documents released to Chumney is a user's manual for the county's version of GEMS. It shows they're using a version of the software that contains the bug known to drop votes, the subject of that 10-month investigation in Ohio in 2008. The software flaw creates exactly the situation described in the e-mails by Young and other officials, one that has been well-known for eight years. Diebold didn't replace the flawed versions outside of Ohio, and for counties to do so on their own was expensive." ([Bloomberg](#), 9/29/2016)

In 2008, ES&S [Diebold] Lied to Ohio Secretary of State About Software Bug That Caused Primary Undervote in 11 Counties. "Ohio Secretary of State Jennifer Brunner sued Diebold following the 2008 primaries after 11 counties using the company's AccuVote-TSX voting machines and GEMS tabulator dropped votes. The company claimed the problem was the result of the antivirus program the counties were using. After a 10-month fight, Diebold conceded the lost votes were the result of a software bug. The bug was fixed in later versions, and more than half of Ohio counties received free or discounted voting machines and software as part of the settlement." ([Bloomberg](#), 9/29/2016)

In Florida, a Major Congressional Race in Florida Imploded After 18,000 Votes From Paperless ES&S iVotronic Machines Went Missing in a Race Decided By Less Than 400 Votes (2006). "But the tipping point came in 2006, when a major congressional race between Vern Buchanan and Christine Jennings in Florida's 13 th District imploded over the vote counts in Sarasota County—where 18,000 votes from paperless machines essentially went missing (technically deemed an "undervote") in a race decided by less than 400 votes. Felten drew an immediate connection to the primary suspect: The ES&S iVotronic machine..." ([Politico](#), 8/5/2016)

A 2002 ES&S Software Error Caused 103,222 Votes to Not Be Counted in The Original Tally in Broward County, Florida. "CNN reported that a software error caused 103,222 votes, cast with ES&S iVotronic paperless machines, to be left uncounted in the original tally. The error was discovered the morning after Election Day. When the missing votes were added, voter turnout for the county was adjusted from 35% to 45%." ([Brennan Center For Justice](#), 2010)

In 2007, Florida's ES&S Machines Were Responsible for a 5% Undervote of Absentee Ballots in the US Senate and US Governor's Race. "In 2007, the Florida Division of Elections listed Orange County as experiencing the highest undervote rates in the state on absentee ballots cast in the 2006 general election for both the U.S. Senate race and the state Governor's race. Alarmed by the exceptionally high rate of undervoted ballots in a major election – nearly 5 percent – the Florida Fair Elections Center's Associate Director contacted the Orange County Elections Administrator, who promised to investigate the issue. According to the Center, Orange County officials responded to the inquiry by stating that their manual inspection of the ballots confirmed that some legitimately cast ballots had not been counted... Bill Cowles, Supervisor of Elections for Orange County noted in an interview with us that the county switched to a different model of ES&S scanner after the 2006 general election." ([Brennan Center For Justice](#), 2010)

An ES&S Software Glitch Led to 32,000 Votes to Not Be Counted on Certain Florida State Amendments. “Two days after Election Day in November 2004, Broward County election officials double-checked election results and discovered that tens of thousands of votes on certain state amendments were not counted. The problem: a “software glitch” in the system used to count the county’s absentee ballots.⁹¹ According to the Palm Beach Post, the software started counting backward after it logged 32,000 votes in a race. Once officials identified the problem and obtained correct vote totals, the newfound votes contributed to a changed result for a statewide gambling amendment and sparked angry calls for a recount.” ([Brennan Center For Justice](#), 2010)

ES&S Machines Led to Nearly 3000 Votes Disappearing in Florida 2018 Recount. “Nearly 3,000 votes effectively disappeared during the machine recount of Florida’s midterm races, according to election records, calling into question whether officials relied on a flawed process to settle the outcome of three statewide contests. With extremely narrow gaps separating candidates in the still-undeclared races for both governor and United States Senate, the results of the machine recount of all votes cast in the Nov. 6 election, posted by the Florida secretary of state’s office, showed 900 fewer votes than those reported in the original statewide tally. The discrepancy was expected to grow by an additional 2,000 votes when updated numbers from Broward County [are added]...Teresa Paulsen, spokeswoman for ES & S, the other company, said machine recounts depend on the same number of ballots being entered into the system. Some ballots could have been torn or damaged after the election, which could have cause a different result in the recount, she said.” ([New York Times](#), 11/17/2018)

In Dallas County, Texas ES&S Machines Failed to Count 41,000 Votes Do to Software Error (1998). “In its maiden run almost two years ago, Dallas County’s new \$ 3.8 million computerized election system overlooked 41,000 votes, one of every eight cast. A software error made it think the votes had already been counted. Thirty elections later, in the March 14 primaries, the county released “final” totals that left out 11,000 votes...“We are concerned that it failed to operate properly in Dallas,” said Ann McGeehan, the state’s director of elections. “This election-reporting system is very clunky.” (*The Dallas Morning News*, Gillman, 4/1/2000)

In the 2008 Presidential Primary, an ES&S Software Error Resulted in Romney Incorrectly Being Declared Winner of Cochise County, Arizona and More Votes Cast than People Registered. “The Douglas Dispatch reported that, in Cochise County, during the 2008 primary presidential race, “a computer glitch that kept counting five polling places over and over again-for five times-caused [a] reporting error” of the election’s results...Consequently, the error resulted in Mitt Romney erroneously being declared winner of Cochise County over John McCain in news reports on the day after the election...Moreover, “the error got worse when the cumulative error went through five updates. It was then realized that the total number of ballots cast according to the wrong report was more than the people registered in the county, Schelling said.” ([Brennan Center For Justice](#), 2010)

ES&S Coding Error Resulted in 2,452 Votes Not Counted in Lackawanna County, Pennsylvania (2009). “The good news is, with paper, we have the ballots.” The large-scale recount was forced by the disclosure last week of a coding error in the county’s computerized vote counters. The error cost city tax collector candidate Bill Courtright and city Councilwoman Janet Evans up to 2,452 straight-party votes. The revelation prompted a flurry of requests for recounts, based partly on fears the error was more widespread, despite Director of Elections Maryann Spellman Young’s assurances to the contrary... Omaha, Neb.-based Election Systems & Software, the machine provider, will lend the

county a new, high-speed vote counter... Party secretary Lance Stange said he is skeptical about the new, high-speed machine recount because Election Systems & Software is providing the machine. "It's from the same company that made the earlier error," he said." (*The Times-Tribune*, Krawczeniuk, 11/13/2009)

ES&S Software Error Caused 94,000 Votes to be Counted Late in North Carolina, Resulting in a Late-Night Lead Change and Complaints Regarding Accuracy (2016). "Similarly, this round of upgrades comes on the heels of concerns regarding the technology used in the 2016 election. In North Carolina, Durham County faced difficulties transferring data off of the memory cards in its vote scanning machine bought from Election Systems & Software. The glitch, the result of memory limitations in the counting software, caused a late-night lead change in the gubernatorial race from then-incumbent Pat McCrory to challenger and eventual victor Roy Cooper, despite the state's website reporting that the county had already completed tallying its votes." (*The News & Observer*, Lewontin, 8/2/2018) (94,000 votes [citation](#))

ES&S Software Error Resulted in 436 Ballots In North Carolina Not Counted (2002). "Problems with voting machines in elections were also making headlines. In 2002 in North Carolina, for example, D.R.E.s made by ES&S failed to record 436 entire ballots during early voting in Wake County, a failure the company attributed to a software bug. Two years later, in Jacksonville, N.C., a D.R.E. made by UniLect lost more than 4,500 ballots when its memory became full and stopped recording; it continued to let voters cast ballots, however, instead of locking up. The incidents that made headlines were disturbing enough, but the real concerns were the ones that weren't being caught." ([New York Times](#), 9/26/2018)

OHIO ES&S SOFTWARE CALLED "HIGHLY DANGEROUS," "CRIMINALLY NEGLIGENT FROM THE STANDPOINT OF DATA SECURITY" AND "INSANELY RISKY" BY ELECTION SECURITY EXPERTS

Attorney Cliff Arnebeck Called the Installation of ES&S Software in Ohio Machines a "Flagrant Violation of the law." His attorney, Cliff Arnebeck, has also referred the case to the Cincinnati FBI for a criminal investigation. Arnebeck says, "It's a flagrant violation of the law. Before you add new software, you need approval of a state board. They are installing an uncertified, suspect software patch that interfaces between the a county's vote tabulation equipment and state tabulators." He adds, "This may be criminal conduct. If they're not doing something wrong, why are they covering it up?" ([Huffington Post](#), 1/23/2014)

In 2014, Free Press Editor-In-Chief Robert Fittrakis Filed a Lawsuit Against ES&S and the Ohio Secretary of State To Halt the Use of Secretly Installed, Unauthorized "Experimental" Voting Machine Software. "Those worries about a rigged election were given new urgency today as The Ohio-based Free Press editor-in-chief Robert Fittrakis, also a Green Party candidate for Congress, announced plans to file a lawsuit later today seeking an immediate injunction against Ohio Secretary of State Jon Husted and the ES&S manufacturer to halt the use of secretly installed, unauthorized "experimental" software in 39 counties' tabulators in an alleged violation of state election law." ([Huffington Post](#), 1/23/2014)

In Sworn Declaration, Election Security Expert Jim March Called ES&S Custom Software Update in Ohio Voting Machines “Highly Dangerous.” “For a number of reasons, I believe that this custom software is not necessary for the conduct of elections and is in fact highly dangerous – the presence of this software significantly reduces the odds that the election results (on a county or statewide level) will be illegally and/or unconstitutionally incorrect. My analysis follows.” ([PDF](#), 11/03/2012)

Election Security Expert Jim March Called ES&S Software “Extremely Dangerous” and Said Deliberate Tampering of Software Would Be “Child’s Play.” “9) What ES&S has chosen to do here is extremely dangerous and exactly what you'd want to do if you wanted to plant a “cheat” onto the central tabulator. Their custom application written in a variant of the COBOL programming language would have full contact with the central tabulator database on both a read and write basis, while running on the same computer as where the “master vote records” are stored. 10) Under this structure a case of accidental damage to the “crown jewels” of the election data is possible. A case of deliberate tampering of that data using uncertified, untested software would be child's play.” ([PDF](#), 11/03/2012)

ES&S Called “Criminally Negligent From a Standpoint of Data Security” by Election Security Expert Jim March in Sworn Declaration. “What they have done instead is criminally negligent just from a standpoint of data security. To double-check the results after this new system is implemented you'd have to go back to the original paper and/or any remaining “poll tapes” from the precincts (“cash register” type paper strips containing that precinct's vote totals). “Poll tapes” from the mail-in vote process may not even exist – most systems feed mail-in votes from scanners straight into the central tabulator with no independent record of the vote. In either case there would need to be public records access to either the poll tapes...or the original paper ballots. There has been widespread media complaints about the access to either sort of public records in Ohio.” ([PDF](#), 11/03/2012)

Election Security Expert Jim March Says ES&S Chosen Methods of Data Collection Are “Unspeakably Stupid, Excessively Complex and Insanely Risky.” “In conclusion, the idea of producing industry-standard .CSV data files of election results is not inherently bad. The method of execution chosen however is unspeakably stupid, excessively complex and insanely risky. In medical terms it is the equivalent of doing open heart surgery as part of a method of removing somebody's hemorrhoids. Whoever came up with this idea is either the dumbest Information Technology “professional” in the US or has criminal intent against the Ohio election process and if I were to guess it would be the latter.” ([PDF](#), 11/03/2012)

Ahead of 2019 Elections, ES&S Has Failed to Install Software Patch Needed for Voting Machines Across Ohio Counties. “[ES&S] which currently supplies the sign-in equipment voters use at their polling location, has said it would provide a software update to make the equipment compatible with recently ordered voting machines. But ES&S has been behind on compliance of its pledge, which has put some election boards across the state in a bind...getting it installed and being trained on operation, the [Hancock County] board’s motion Monday requires a decision from ES&S and the Secretary of State’s office on systems compatibility by July 12...If a decision hasn’t been received, the board authorized contacting Knowlnk, a St. Louis, Missouri-based company, to provide the “poll pad” equipment.” ([The Courier](#), 6/25/2019)

In 2005, ES&S Surprised Small Ohio County With \$40,000 Per Year Service Fee for Election Software Written in 1996.

“When Allen County, Ohio, replaced its old voting machines in 2005 with equipment from ES&S, officials didn’t realize they’d also be stuck with a service fee of \$40,000 per year to help run an election system that handled about 70,000 votes. “When we found out the cost, our jaws just about hit the floor,” says Ken Terry, who was election director there until this year. To top it off, Terry discovered that the county was paying top dollar for antiquated technology. It wasn’t until the machines were purchased, and in place, that county officials realized their new system ran on software written in 1996.” ([Bloomberg](#), 9/29/2016)

ES&S HAS CONSISTENTLY DEMONSTRATED A SYSTEMATIC DISREGARD FOR BASIC SECURITY BEST PRACTICES AND A COMPLETE LACK OF COMPETENCE IN THE MANUFACTURING OF RELIABLE VOTING MACHINES

In May 2019, A Critical Firewall Vulnerability that Allowed Attackers to “Fully Compromise” Device Networks, Was Found in ES&S Voting Machines.

“The first is a bug in Cisco’s IOS operating system—not to be confused with Apple’s iOS—which would allow a hacker to remotely obtain root access to the devices. This is a bad vulnerability, but not unusual, especially for routers.... The second vulnerability, though, is much more sinister. Once the researchers gain root access, they can bypass the router’s most fundamental security protection...In practice, this means an attacker could use these techniques to fully compromise the networks these devices are on...“That means we can make arbitrary changes to a Cisco router, and the Trust Anchor will still report that the device is trustworthy. Which is scary and bad, because this is in every important Cisco product. Everything.” ([Wired](#), 5/13/19)

Cisco Security Advisory Lists Firewall “ASA 5506-X” as First Affected Product.

([Ciscos.com](#), 5/13/2019)

The ES&S Firewall Systems “ASA-5506-X”, Made by Cisco, Was

Used by ES&S in Michigan¹, Florida², and Iowa³. (¹[MI Contract](#), 3/1/2017) (²[FL Certification](#), 2/9/2012) (³[State of Iowa](#), 9/18/18)

Did ES&S Properly Warn States and Counties that their Voting Machines Could Be “Fully Compromised?” Has ES&S Installed the Recommended Software Patch in Every Single Affected Voting Machine?

Nearly Every Make and Model of Voting Machine Created in the Last 15 Years Is Vulnerable to Hacking.

It was just another example of something that Eckhardt and other experts had suspected for many years: that many critical election systems in the United States are poorly secured and protected against malicious attacks. In the 15 years since electronic voting machines were first adopted by many states, numerous reports by computer scientists have shown nearly every make and model to be vulnerable to hacking. ([New York Times](#), 2/21/2018)

As of September 2018, ES&S Failed to Fix Massive Security Flaw in Scanners Originally Discovered 11 Years Ago—Still Selling Scanners on Website.

An uncorrected security flaw in a vote-counting machine used in 23 U.S. states leaves it vulnerable to hacking 11 years after the manufacturer was alerted to it, security researchers say. The M650 high-speed ballot scanner is made

by Election Systems & Software, the nation's leading elections equipment vendor. The vulnerability was the most serious noted in voting equipment in a report Thursday... "If successfully hacked by someone intent on changing vote totals in a swing-state county, "it could flip the Electoral College," [Jake Braun] said... ES&S did not respond when asked by The Associated Press why it had not corrected the Zip drive vulnerability despite knowing about it for more than a decade. It also did not say whether it continues to sell the M650, which was listed on its website product offerings as recently as last month." (*St. Louis Post-Dispatch*, Bajak, 11/28/2018)

Election Expert on ES&S 'What I've seen in the past 10 years is that the vendors have absolutely fumbled every single attempt in security.' "What I've seen in the past 10 years is that the vendors have absolutely fumbled every single attempt in security," says Jacob D. Stauffer, vice president of operations for Coherent Cyber, who has conducted voting-machine security assessments for California's secretary of state for a decade. In a report Stauffer and colleagues published last year about their recent assessment of ES&S machines, they found the voting machines and election-management systems to be rife with security problems." ([New York Times](#), 2/21/2018)

ES&S's New Barcode-Ballot Producing Machines Called "A Ruse" that "Makes a Mockery of Notion that the Ballot is 'Voter-Verifiable.' "The new machines being peddled by companies like Election Security & Software (ES&S), the nation's biggest vendor of voting technology, are designed to give the impression of being "voter-verifiable." But it's a ruse. The machines produce a so-called "paper ballot," which voters can use to verify a text printout of their votes if they take the time. But it's not the text the voter is reading and reviewing, but the barcode beneath, that is actually tallied electronically as their vote... Elections officials can't, either. The barcode-based setup "makes a mockery of the notion that the ballot is 'voter-verifiable,'" agreed Duncan Buell, a computer science professor at the University of South Carolina, because "what the voter verifies is not what is tallied." ([The New Republic](#), 3/06/2019)

University of Iowa Computer Scientist Slammed ES&S For "Mediocre Programming," "Insufficient Pre-Election Testing," and a Complete Lack of "Security Conscious" in Any Phase of Their Design. "University of Iowa computer scientist Douglas Jones said both incidents reveal mediocre programming and insufficient pre-election testing. And voting equipment vendors have never seemed security conscious "in any phase of their design," he said." ([AP News](#), 10/29/2018)

ES&S Sold 22,619 Faulty Voting Machines That Lose Calibration Throughout Election Day Causing "Vote Flipping." "There is a real chance that voters using iVotronic machines in your state will experience 'vote flipping' similar to that experienced by voters in West Virginia," the letter said. "What they've seen is calibration drift on a unit," Merriman said. "They're fine in the morning, but by afternoon they're starting to lose their calibration." The phenomenon is described in a federal lawsuit filed in November 2005 by Bergquist Co., which makes touch screens for ES&S... It described how air pockets between layers of the screen and residual acid in an ink compound were causing the touchscreens to malfunction..." "Ultimately, Bergquist determined that the dielectric ink, which had caused the sudden 'out-of-calibration' problems, had been used in 22,619 touch screens sold by Pivot and incorporated in voting machines, and thus every screen had failed and required replacement." ([Salina Journal](#), 4/10/2009)

2018 Report Commissioned by California Secretary of State Found 115 Critical and Important Software Patches to Be Missing and 176 Instances of Server Misconfigurations on ES&S Machines. Please See Appendix A. ([ES&S Security Test Report](#), 8/28/2017)

ES&S Misconfigured Windows 7 Software 96 Times on Machines They Chose to Provide to California Secretary of State for Security Testing. Please See Appendix A. ([ES&S Security Test Report](#), 8/28/2017)

The AP Said ES&S Faced No Significant Oversight and Operated Under a Shroud of Financial and Operational Secrecy. “A trio of companies — ES&S of Omaha, Nebraska; Dominion Voting Systems of Denver and Hart InterCivic of Austin, Texas — sell and service more than 90 percent of the machinery on which votes are cast and results tabulated. Experts say they have long skimmed on security in favor of convenience, making it more difficult to detect intrusions such as occurred in Russia’s 2016 election meddling. The businesses also face no significant federal oversight and operate under a shroud of financial and operational secrecy despite their pivotal role underpinning American democracy.” ([AP News](#), 10/29/2018)

In 2017, Rigorous Scrutiny of Voting Systems Found Multiple Vulnerabilities in ES&S’s Electionware System That Could Allow Intruders to Erase All Recorded Votes. “California conducts some of the most rigorous scrutiny of voting systems in the U.S. and has repeatedly found chronic problems with the most popular voting systems. Last year, a state security contractor found multiple vulnerabilities in ES&S’s Electionware system that could, for instance, allow an intruder to erase all recorded votes at the close of voting. ([AP News](#), 10/29/2018)

Security Researchers Discovered Critical Vulnerabilities In ES&S Software That Would Allow Attackers to Seize Control of System. “Around this same time, security researchers discovered a critical vulnerability in pcAnywhere that would allow an attacker to seize control of a system that had the software installed on it, without needing to authenticate themselves to the system with a password. And other researchers with the security firm Rapid7 scanned the internet for any computers that were online and had pcAnywhere installed on them and found nearly 150,000 were configured in a way that would allow direct access to them. It’s not clear if election officials who had pcAnywhere installed on their systems, ever patched this and other security flaws that were in the software.” ([MotherBoard](#), 7/17/2018)

ES&S Installed Third Party Software On Its Election System During the Same Time Period That Software Was Hacked. “In 2006, the same period when ES&S says it was still installing pcAnywhere on election systems, hackers stole the source code for the pcAnywhere software, though the public didn’t learn of this until years later in 2012 when a hacker posted some of the source code online, forcing Symantec, the distributor of pcAnywhere, to admit that it had been stolen years earlier. Source code is invaluable to hackers because it allows them to examine the code to find security flaws they can exploit.” ([MotherBoard](#), 7/17/2018)

ES&S Used Easily Hackable Cell Phone Modems to Upload Election Night Results. “The ES&S model DS200 optical-scan voting machine has a cell-phone modem that it uses to upload election-night results from the voting machine to the “county central” canvassing computer. We know it’s a bad idea

to connect voting machines (and canvassing computers) to the Internet, because this allows their vulnerabilities to be exploited by hackers anywhere in the world...So, in summary: phone calls are not unconnected to the Internet; the hacking of phone calls is easy (police departments with Stingray devices do it all the time); and even between the cell-towers (or land-line stations), your calls go over parts of the Internet.” ([Freedom to Tinker](#), 2/22/2018)

Despite Hackers Ability to Change Votes In ES&S Machines, ES&S Has No Way to Audit Its Own Firmware, So Corrupt Firmware Would Remain Indefinitely. “In all three cases, the practical implication of this attack would be to allow attackers to change votes and hence election outcomes. This attack is potentially persistent, because unless iVotronic machines are audited before future elections, it is plausible that the firmware will remain on the iVotronic system indefinitely. According to the EVEREST report, ES&S has no way to audit its own firmware, so this means that persistently corrupted firmware is the rule, not the exception.” ([David Cahn – University of Pennsylvania](#), 4/26/2017)

The 30,000 ES&S Optical Scanners Across 43 States Are “Naively Designed” and Allow For Attacks That Could Infect Central Unity Systems Used To Count Votes Countywide. “ES&S M100 Optical Scan voting machines are paper ballot tabulators. 30,000 M100 Optical Scan machines are used to count votes in 43 states. Due to their design, the attack surface for these machines is smaller than that of touch screen voting systems. Since there is no user interface, regular voters might find it difficult to attack the M100. Not so for poll workers; M100 machines are naively designed, allowing for malware and firmware attacks that could, at best, alter the voting results for a single precinct, and at worst infect the central Unity system used to count countywide votes. ([David Cahn – University of Pennsylvania](#), 4/26/2017)

ES&S Did Not Hire A Data Security Officer Until April of 2018. “ES&S hired its first chief information security officer in April. None of the big three vendors would say how many cybersecurity experts they employ. Stimson said that “employee confidentiality and security protections outweigh any potential disclosure.” ([AP News](#), 10/29/2018)

An Election Specialist Said the ES&S Breach “Raises A Lot of Questions About Their Ability To Keep Both the Voting Systems They Run and Their Own Networks Secure.” “The implications of the exposure are much broader than Chicago because Election Systems & Software is the largest vendor of voting systems in the United States, said Susan Greenhalgh, an election specialist with Verified Voting, a non-partisan election integrity non-profit. “If the breach in Chicago is an indicator of ES&S's security competence, it raises a lot of questions about their ability to keep both the voting systems they run and their own networks secure,” she said.” ([USA Today](#), 08/18/2017)

Election Technology Expert Said It Would Be “Unprofitable” For ES&S to Build Truly Secure Systems. “In much of the nation, especially where tech expertise and budgets are thin, the companies effectively run elections either directly or through subcontractors. “They cobble things together as well as they can,” University of Connecticut election-technology expert Alexander Schwartzman said of the industry leaders. Building truly secure systems would likely make them unprofitable, he said.” ([AP News](#), 10/29/2018)

ES&S Passed ProCircular Testing Yet Barred Company from Releasing Any Details. “ProCircular’s team spent several weeks conducting penetration testing on the hardware,

software, and way the device performed. The firm found the [ES&S] devices to be, in their words, “reliable and secure.”... ProCircular did not release further details on the report due to a confidentiality agreement with ES&S. Such agreements are standard when a company undergoes a penetration test.” ([Cyberscoop](#), 4/24/2019)

Cybersecurity Reporter, Eric Geller, Called the Brief Statement by ProCircular, Published Without Data, “The Exact Opposite of What Independent Experts Have Been Recommending for Decades. “Does ES&S actually think a brief statement from a company that can’t publish its test results will reassure anyone? This is the exact opposite of what independent experts have been recommending for decades.” ([Twitter](#), 4/24/2019)

Microsoft Will Stop Providing Free Support for ES&S Certified Windows 7 Software on January 14th. “That’s significant because Windows 7 reaches its “end of life” on Jan. 14, meaning Microsoft stops providing technical support and producing “patches” to fix software vulnerabilities, which hackers can exploit. In a statement to the AP, Microsoft said Friday it would offer continued Windows 7 security updates for a fee through 2023.” ([AP](#), 7/13/2019)

ES&S May Not Be Able To Certify Windows 10 Before 2020 Primaries. “For many people, the end of Microsoft 7 support means simply updating. However, for election systems the process is more onerous. ES&S and Hart don’t have federally certified systems on Windows 10, and the road to certification is long and costly, often taking at least a year and costing six figures...Though ES&S is testing a new system it’s unclear how long it will take to complete the process — federal and possible state recertification, plus rolling out updates — and if it will be done before primaries begin in February.” ([AP](#), 7/13/2019)

ES&S Did Not Complete Windows 7 Certification (Released in 2009) Until March 2019. “ES&S, the nation’s largest vendor, completed its latest certification four months ago, using Windows 7. Hart’s last certification was May 29 on a Windows version that also won’t be supported by November 2020.” ([AP](#), 7/13/2019)

ES&S LARGE-SCALE NEGLIGENCE EXPOSED PERSONAL DATA OF MILLIONS OF VOTERS, LEFT TENS OF THOUSANDS OF NAMES OFF ROLLS AND LED TO MASSIVE DELAYS IN VOTE COUNTS ACROSS THE COUNTRY

In Chicago, ES&S Negligence Exposed Personal Data of 1.8 Million Voters, Including Partial Social Security Numbers and Driver’s License Information in 2017. “Names, addresses, dates of birth and other information about Chicago’s 1.8 million registered voters was left exposed and publicly available online on an Amazon cloud-computing server for an unknown period of time, the Chicago Board of Election Commissions said. The database file was discovered August 11 by a security researcher at Upguard, a company that evaluates cyber risk. The company alerted election officials in Chicago on August 12 and the file was taken down three hours later. The exposure was first made public on Thursday.” ([USA Today](#), 08/18/2017)

In Alabama, ES&S Used Critically Flawed and Unsecured Wireless Connections In Voting Machines Until the State Forced Them To Remove Wireless Connections Last Year. “For instance, industry leader ES&S sells vote-tabulation systems equipped with cellular modems, a feature that experts say sophisticated hackers could exploit to tamper with vote counts. A few states ban such wireless connections; in Alabama, the state had to force ES&S to remove them from machines ordered for one of its counties earlier this year. “It seemed like there was a lot more emphasis about how cool the machines could be than there was actual evidence that they were secure,” said John Bennett, the Alabama secretary of state’s deputy chief of staff.” ([AP News](#), 10/29/2018)

In Los Angeles County, ES&S “Sloppy System Integration” Left 118,000 Names Off Printed Voter Rolls In 2018. “During this year’s primary elections, ES&S technology stumbled on several fronts. In Los Angeles County, more than 118,000 names were left off printed voter rolls. A subsequent outside audit blamed sloppy system integration by an ES&S subsidiary during a database merge.” ([AP News](#), 10/29/2018)

In 2008, Florida’s ES&S DS200 Machines Had an Overvote Rate on Election Day that Was 18 Times Greater Than Any Other System in Florida. “A study from the Florida Fair Elections Center shows that counties using the ES&S DS200, which in the event of an overvote displayed a confusing message and did not automatically reject a ballot, had an overvote rate on Election Day 2008 that was as much as 18 times that of systems used in other Florida counties.” ([Brennan Center For Justice](#), 2010)

ES&S Failed to Notify Elections Officials in Pulaski County, Arkansas that Screens Would Appear Distorted for Voters Over 6ft Tall, Potentially Causing Them to Choose Incorrect Candidate (2006). “During early voting in the May primary, several voters complained of problems with an ES&S touch screen DRE. According to a local newscast, Pulaski County election officials tested the machine and determined that the machine was not broken; an optical illusion perceived by voters who were over six feet tall caused the problem. Officials determined that the angle at which particularly tall voters viewed the screen caused them to believe that they were voting for the candidate below the one for whom a vote was recorded... a company employee told her that they were already aware of optical illusion problems experienced by tall voters... Officials were livid at the thought that ES&S could have known about the problem and failed to warn them.” ([Brennan Center For Justice](#), 2010)

ES&S Sent Madison County, Indiana 7,400 Faulty Ballots, Then Blamed County For Not Testing The Ballots First (2008). “The Herald Bulletin reported “that as many as 7,400 of the 12,000-some ballots used for early voting could not be counted by the machines. As it turns out, the coding on that portion of the early ballots was in the wrong position on the paper, tripping up the machines.” According to an editorial in the paper, “an official from Omaha-based Election Systems & Software, which provided the counting system, seemed to acknowledge that the company had sent the county ballots that wouldn’t work. But the county should take some blame too for not taking the precaution of testing the new set of ballots when they arrived.” ([Brennan Center For Justice](#), 2010)

ES&S Sent Tennessee County Incorrect Early Vote File, More than 10,000 Names Missing (2014). “Last Tuesday, as Davidson County voters were casting their ballots in local judicial primaries, election officials realized there was a problem - more than 10,000 people could have voted twice, and no one working the polls would have known to stop them...After more than 13,000 people voted early for the

May elections, the commission sent those records to ES&S. But when the files came back, to be entered into the EPBs for use on election day, Wall says they only contained the records of a little more than 2,000 voters. The missing records meant that more than 10,000 early voters could have shown up again on Election Day and voted a second time without being detected at the time.” (*Nashville Scene*, Hale, 5/12/2014)

In Kansas, ES&S Did Not Do Any Audit After Software Error Led To Kansas’ Most Populous County’s Vote Count Being Stalled For 13 Hours in 2018. “No such audit was done in Kansas’ most populous county after a different sort of error in newly installed ES&S systems delayed the vote count by 13 hours as data uploading from thumb drives crawled.” ([AP News](#), 10/29/2018)

US SENATORS EXPRESS NATIONAL SECURITY CONCERNS AFTER ES&S LIED TO FEDERAL LAWMAKERS, REFUSED TO REVEAL WHICH STATES WERE SENT CRITICALLY FLAWED MACHINES, & VIGOROUSLY FOUGHT ATTEMPTS TO REVEAL RELIABILITY INFORMATION

ES&S Revealed it is Owned by Private Equity Firm McCarthy Group, LLC. “Pursuant to the recently modified State of North Carolina Election Systems Certification Program, the following entities and/or individuals own a 5% or greater interest or share in ES&S, any subsidiary company of ES&S, and ES&S’ parent company. Government Systems, Software & Services, Inc. owns 100% of the membership units of Election Systems & Software... Please be advised that McCarthy Group, LLC owns a controlling interest in Government Systems, Software, & Services, LLC.” ([PBS.TWIMG](#), 6/21/2019)

In Letter to ES&S & Other Vendors, US Senators Warn Decades Old Voting Machine Vulnerabilities Are a Significant National Security Concern. “Despite the progress that has been made, election security experts and federal and state government officials continue to warn that more must be done to fortify our election systems. Of particular concern is the fact that many of the machines that Americans use to vote have not been meaningfully updated in nearly two decades. Although each of your companies has a combination of older legacy machines and newer systems, vulnerabilities in each present a problem for the security of our democracy and they must be addressed.” ([Office of Senator Amy Klobuchar](#), 3/26/2019)

US Senators Call Market for Election Equipment “Broken,” Claim ES&S/Others of Producing Vulnerable Voting Machines. “In other words, the fact that VVSG 2.0 remains a work in progress is not an excuse for the fact that our voting equipment has not kept pace both with technological innovation and mounting cyber threats...The fact that you continue to manufacture and sell outdated products is a sign that the marketplace for election equipment is broken.” ([Office of Senator Amy Klobuchar](#), 3/26/2019)

US Senators Conclude “Voter-Verifiable Paper Ballots” Are Basic Necessities For A Reliable Voting System. “There is a consensus among cybersecurity experts regarding the fact that voter-verifiable paper ballots and the ability to conduct a reliable audit are basic necessities for a reliable voting system. Despite this, each of your companies continues to produce some machines without paper ballots” ([Office of Senator Amy Klobuchar](#), 3/26/2019)

Senator Ron Wyden Said ES&S has “Figured Out a Way to be Above the Law” and Georgia Showed the Company is “Accountable to Nobody.” “We’re up against some really entrenched, powerful interests, who have really just figured out a way to be above the law,” he said. “There is no other way to characterize it.” Furthermore, Wyden said, voting machine vendors have “been able to hotwire the political system in certain parts of the country.” He noted that newly elected Georgia Gov. Brian Kemp picked the top lobbyist for the voting giant Election Systems & Software as his deputy chief of staff. The companies, he said, “are accountable to nobody.” ([Politico](#), 3/14/19)

Senator Ron Wyden Demanded ES&S Explain “Suspect Claims” the Company Made to the League of Women Voters of South Carolina that ES&S Machines Have Never Been Breached. “I write to seek an explanation of suspect claims that Election Systems and Software (ES&S) has made regarding the security of your voting machines. In a January 15, 2019, letter to the League of Women Voters of South Carolina, ES&S wrote that ‘no ES&S machine has ever been breached or comprised in an election.’ Your company’s letter does not explain the basis for its assessment that its voting machines have a spotless cybersecurity track record.” ([Office of Senator Ron Wyden](#), 4/2/2019)

Senator Ron Wyden Said Vendors like ES&S had “Sketchy Ethics,” “Lie to Public Officials,” and “Repeatedly Gouge Taxpayers.” “Sen. Ron Wyden (D-Ore.) on Thursday attacked the small but powerful group of companies that controls the production of most voting equipment used in the U.S. ‘The maintenance of our constitutional rights should not depend on the sketchy ethics of these well-connected corporations that stonewall the Congress, lie to public officials, and have repeatedly gouged taxpayers, in my view, selling all of this stuff,’ Wyden said...” ([Politico](#), 3/14/19)

ES&S Added Two New Lobbying Firms Last Fall in Anticipation of Increasing Pressure from Lawmakers to Protect Elections. “Voting machine manufacturers are increasing their Capitol Hill presence as lawmakers demand they do more to protect U.S. elections against foreign hackers ... In October, ES&S hired Peck Madigan Jones, and paid the firm \$80,000 during the last three months of 2018. The company also reported hiring the lobbying firm Vectre Corp.” ([Bloomberg](#), 4/1/2019)

ES&S Initially Lied When Asked If It Installed Third Party Hackable Software on Election-Management Systems Over Six Years. “The nation’s top voting machine maker has admitted in a letter to a federal lawmaker that the company installed remote-access software on election-management systems it sold over a period of six years, raising questions about the security of those systems and the integrity of elections that were conducted with them. In a letter sent to Sen. Ron Wyden (D-OR) in April and obtained recently by Motherboard, Election Systems and Software acknowledged that it had “provided pcAnywhere remote connection software ... to a small number of customers between 2000 and 2006,” which was installed on the election-management system ES&S sold them. The statement contradicts what the company told me and fact checkers for a story I wrote for the New York Times in February. At that time, a spokesperson said ES&S had never installed pcAnywhere on any election system it sold.” ([MotherBoard](#), 7/17/2018)

ES&S Refused to Tell Federal Lawmakers Which States/Counties Were Sold Critically Flawed Voting Machines. “He notes that election officials who purchased the systems likely were not aware of the potential risks they were taking in allowing this and didn’t understand the threat landscape to make

intelligent decisions about installing such software...Although Wyden's office asked ES&S to identify which of its customers were sold systems with pcAnywhere installed, the company did not respond. ES&S would only say that it had confirmed with customers who had the software installed that they "no longer have this application installed."...As late as 2011 pcAnywhere was still being used on at least one ES&S customer's election-management system in Venango County, Pennsylvania." ([MotherBoard](#), 7/17/2018)

ES&S Refused to Comment to Federal Lawmakers on Whether Critical Security Flaws in Voting Machine Software Were Adequately Patched. "It's not clear if election officials who had pcAnywhere installed on their systems, ever patched this and other security flaws that were in the software...But when Wyden's office asked in a letter to ES&S in March what settings were used to secure the communications, whether the system used hard-coded or default passwords and whether ES&S or anyone else had conducted a security audit around the use of pcAnywhere to ensure that the communication was done in a secure manner, the company did not provide responses to any of these questions." ([MotherBoard](#), 7/17/2018)

In Wisconsin, ES&S Filed A Lawsuit Demanding Presidential Campaigns Sign NDA's to Prevent Public Discussion of Machine Reliability Following Election Issues. "Electronic Systems & Software and Dominion Voting Systems supply most of the machines used in Wisconsin elections. The two companies filed a lawsuit in April demanding the nondisclosure agreement prohibit Stein's auditors and campaign from publicly discussing any conclusions and criticisms stemming from the review. The companies argued public discussion amounts to an unauthorized use or disclosure of proprietary information." ([The Journal Times](#), 1/30/2019)

In Colorado, ES&S Refused to Seek Certification After the State Required Vulnerability Testing of Voting Machines. "In an April 2014 meeting with Colorado elections officials, ES&S objected to a new state requirement for vulnerability testing because it didn't allow for the results to be kept secret, Colorado Deputy Secretary of State Suzanne Staiert said in an interview. She said the company ultimately didn't seek certification because the system it was offering didn't meet state requirements. ES&S did not directly respond to a query about this incident. A company spokeswoman said a review of company correspondence found no sign that it resisted the testing requirement, although it did "ask clarifying questions." ([AP News](#), 10/29/2018)

The Brennan Center For Justice Said there are "More Federal Regulations for Ballpoint Pens & Magic Markers Than There Are For Voting Systems." "In contrast to other sectors, particularly those that the federal government has designated 'critical infrastructure,' there is almost no federal oversight of private vendors that design and maintain the systems that allow us to determine who can vote, how they vote, what voters see when they cast their vote, how votes are counted, and how those vote totals are communicated to the public," [the Brennan Center for Justice's Lawrence] Noren told Congress recently in a testimony. "In fact, there are more federal regulations for ballpoint pens and magic markers than there are for voting systems and other parts of our federal election infrastructure." ([Sludge](#), 6/10/2019)

Following Pressure from Lawmakers, ES&S CEO Tom Burt Said the Company Would No Longer Sell Paperless Voting Machines as Primary Device for Casting Ballots. “Voting machine maker ES&S has said it “will no longer sell” paperless voting machines as the primary device for casting ballots in a jurisdiction. ES&S chief executive Tom Burt confirmed the news in an op-ed. TechCrunch understands the decision was made around the time that four senior Democratic lawmakers demanded to know why ES&S, and two other major voting machine makers, were still selling decade-old machines known to contain security flaws.” ([TechCrunch](#), 6/9/2019)

After Facing Criticism for Denouncing Machine Vulnerabilities, ES&S CEO Called for Legislation Mandating Stronger Election Machine Testing Programs. “The chief executive also called on Congress to pass legislation mandating a stronger election machine testing program. Burt’s remarks are a sharp turnaround from the company’s position just a year ago, in which the election systems maker drew ire from the security community for denouncing vulnerabilities found by hackers at the annual Defcon conference. ([TechCrunch](#), 6/9/2019)

ES&S CEO Tom Burt Also Called For “Physical Paper Records of Votes” (*not the same as hand-marked paper ballots*).** “Second, we must have physical paper records of votes. Our company, Election Systems & Software, the nation’s leading elections equipment provider, recently decided it will no longer sell paperless voting machines as the primary voting device in a jurisdiction. That’s because it is difficult to perform a meaningful audit without a paper record of each voter’s selections. Mandating the use of a physical paper record sets the stage for all jurisdictions to perform statistically valid postelection audits. ([Roll Call](#), 6/7/2019)

Critics Called the ES&S Pivot New “Marketing” “After Years of Selling Voting Equipment It Knew Was Insecure.” “But critics say Election Systems & Software’s open pivot to paper is simply marketing, after the company saw that paperless machines were on the way out. “After years of selling voting equipment that it knew was insecure, and fighting tooth and nail against real election security, ES&S is finally admitting that paper ballots are the most secure system currently available,” Sen. Ron Wyden, whose PAVE Act is one of the strictest security bills introduced in the Senate, told CNN in a statement.” ([CNN](#), 6/19/2019)

Senator Wyden Said ES&S Should Tell Its “Friends in Georgia” to Stop Standing in the Way of Legislation to Help Protect American Democracy. “If it is serious about this change of heart, ES&S would tell its friends in Georgia and Speaker McConnell to stop standing in the way of the PAVE Act’s common-sense requirements to protect American democracy,” the Oregon Democrat said. ([CNN](#), 6/19/2019)

ES&S Paid Lobbying Firm Peck Madigan Jones \$150,000 to Lobby House and Senate Members. ES&S hired lobbying firm Peck Madigan Jones in Oct. 2018 and paid it a combined \$150,000 to lobby the U.S. Senate and House of Representatives in the fourth quarter of 2018 and the first quarter of 2019. ([Sludge](#), 6/10/2019)

ES&S Lobbyists Donated to Mitch McConnell—Who is “Single-Handedly” Standing in the Way of Any Election Security Legislation. “Emily Kirlin, a lobbyist for Peck Madigan Jones who lobbies for ES&S on election security and H.R. 1, gave McConnell’s campaign committee \$1,000 on February 19, and her colleague who works with her on the contract, Jen Olson, gave McConnell \$1,000 on March 4.

“It’s not surprising to me that Mitch McConnell is receiving these campaign contributions,” the Brennan Center for Justice’s Lawrence Noren told Sludge. “He seems single-handedly to be standing in the way of anything passing in Congress around election security...” ([Sludge](#), 6/10/2019)

Public Citizen Called the ES&S Contributions to McConnell “A Reward from the Industry for Letting Them Off the Hook.” “Mitch McConnell’s conflicts of interest in blocking any and all election security legislation is not only shameful, it is placing our democracy at risk,” Craig Holman, government affairs lobbyist at Public Citizen, told Sludge. “The conflicts of interest arise from more than the campaign contributions he is receiving from voting machine vendors—contributions which certainly appear to be a reward from the industry for letting them off the hook—but it is also a self-serving act for strictly partisan purposes. ([Sludge](#), 6/10/2019)

Ballot Marking Devices Cost About 3x As Much as Truly Paper-Based Systems, Says Election Security Expert in Congressional Testimony. “According to testimony from Alex Halderman, Professor of Computer Science and Engineering at the University of Michigan, equipping a precinct with ballot-marking electronic devices costs about three times as much as equipping it with a truly paper-based system along with a dedicated electronic device for voters with disabilities. “Fortunately, the most cost-effective approach is also the most secure: hand-marked paper ballots counted using optical scanners,” Halderman stated. ([Sludge](#), 6/10/2019)

ES&S INDIANA CONTRACT TERMINATED AFTER INVESTIGATION REVEALS ES&S VIOLATED INDIANA STATE LAW, LIED TO ELECTION OFFICIALS, AND WERE RESPONSIBLE FOR ERRORS RESULTING IN LONG WAIT TIMES, VOTER ANXIETY, DISCOURAGED VOTERS, AND EMBARRASMENT

Johnson County Terminated Contract with ES&S After State Investigation Determined ES&S Responsible for Technical Issues that Triggered Long Lines in 2018. What struggled to work were the electronic poll books used to check a voter’s registration, triggering long lines at polling stations. A state investigation determined that the vendor for the e-poll books, Election Systems & Software (ES&S), was responsible for the technical issue, and the Johnson County election board ultimately voted to terminate the contract. ([The Hill](#), 3/24/19)

Johnson County Clerk Said the Community Had Lost Trust in ES&S. “Trena McLaughlin, the county clerk for Indiana’s Johnson County who took office after the November vote, told The Hill that the election board decided to terminate its contract with ES&S because the community had lost trust in the vendor. “We have had a lot of people asking, ‘should we be using ES&S?’” she said.” ([The Hill](#), 3/24/19)

ES&S Issues Resulted in Voter Anxiety, Discouraged Voting, and Brought Embarrassment and Negative Publicity to Johnson County. “The problems which occurred in Johnson County was a source of negative publicity for the County. In addition to embarrassment, the more important impact was on voters who did not understand what was occurring and this likely created voter anxiety, impacted confidence in the electoral process, and probably discouraged voters from continuing to wait to cast a ballot. The work around offered on Election Day was not in compliance with the Indiana Election Code.” ([Voting System Technical Oversight Program Report](#), 12/31/2018)

Indiana Officials Called Election Day Issues “Unacceptable” and Said the Responsibility “Rests on the Shoulders of ES&S.” “The situation which occurred in Johnson is unacceptable for any Indiana electronic poll book vendor. The responsibility for what occurred rests on the shoulders of ES&S, because they opted for a limited WAF instance configuration with Microsoft Azure after switching from Amazon Web Services. The premise that their pre-election load testing adequately predicted election day needs is difficult to accept.” ([Voting System Technical Oversight Program Report](#), 12/31/2018)

ES&S Violated Indiana State Law When It Failed to Report Several System “Anomalies” Prior to Election Day. “The VSTOP investigators also concluded that ES&S failed to report several system “anomalies” that occurred prior to election day, which violates Indiana election law. And, attempts to fix the lagging computer issues on election day also resulted in a violation of state code.” ([CBS4Indy.com](#), 1/09/2019)

ES&S Violated Indiana Law When It Offered County A Work-Around for Its Own Performance Issues. “3. ES&S made a business decision to move from Amazon Web Service (AWS) to Microsoft Azure but did not notify the State of Indiana or VSTOP. 4. ES&S offered Johnson County a work-around to allow voters to be checked in at the vote centers. However, this work-around resulted in electronic poll books not being able to communicate between vote centers in Johnson County. This solution was not in compliance with the Indiana Election Code. 5. ES&S has stated that the Microsoft Azure Web Application Firewall (WAF), which is part of the Application Gateway, is the key reason for the performance issues on Election Day. 6.” ([Voting System Technical Oversight Program Report](#), 12/31/2018)

“After Tests Failed to Predict Election Day Server Needs, ES&S Erased All Logs Prior to Election Day and All Diagnostic Logs For The General Election.” “ES&S misjudged server needs and the impact of WAF instances for Election Day. Pre-election load tests conducted by ES&S did not adequately predict Election Day server needs. The logs for the load tests prior to the primary were not retained. Moreover, diagnostic logs were not retained by Microsoft or by ES&S for the General Election. 8. ES&S admitted, in retrospect, that 7 WAF instances was not sufficient for Election Day.” ([Voting System Technical Oversight Program Report](#), 12/31/2018)

ES&S Lied to Indiana Officials About the Cause of Slow Electronic Poll Books On Election Day. “ES&S initially maintained that the problem with slow electronic poll book performance on Election Day was caused by the Microsoft Azure Web Application Firewall (WAF). It was discovered in responses to VSTOP questions by ES&S, and in subsequent conversations with ES&S, that the problem was caused by the limited number of instances in the WAF that ES&S secured through Microsoft Azure for electronic poll book data traffic.” ([Voting System Technical Oversight Program Report](#), 12/31/2018)

Indiana Officials Believe ES&S Issues May Have Occurred in All Counties On Election Day In 2018. “The anomaly report from ES&S, required by law, was limited in scope concerning the issues encountered. Issues may have also occurred in all ES&S counties on Election Day as well as during early voting (see Appendix A).” ([Voting System Technical Oversight Program Report](#), 12/31/2018)

ES&S Did Not Have Their Systems Properly Set Up To Handle High Voter Turnout. “The VSTOP report claims Johnson County’s election software vendor, ES&S inadequately anticipated server needs

on election day, and did not have their systems properly set up to handle the high voter turnout seen around the county.” ([CBS4Indy.com](https://www.cbs4indy.com), 1/09/2019)

In 2018, ES&S Pollbooks Did Not Meet Performance Expectations in Indiana and Resulted In Longer Wait Times. “The ES&S ExpressPoll EZRoster 3.2.2.1 did not meet performance expectations at vote centers in Johnson County, Indiana on Election Day, November 6, 2018. 2. The ExpressPoll EZ Roster 3.2.2.1 performance issues resulted in longer than expected wait times for voters.” ([Voting System Technical Oversight Program Report](#), 12/31/2018)

Information Assurance Compliance

Using the NIST Security Content Automation Protocol (SCAP), all Electionware servers and workstations were scanned for misconfigurations in accordance with US federal IA standards. These standards conform to mitigating known vulnerabilities and hardening target systems on a US government network.

The following table presents a summary of patches missing on the operating system and misconfigurations on each class (workstation or server) of systems in the Electionware suite.

Electionware Servers

Missing Operating System Patches	
Critical	17
Important	49
Moderate	2
Unrated	8

SCAP Misconfigurations	
Windows 2008 R2 STIG³	46
Firewall STIG Configuration	3
.NET Framework 4 STIG Configuration	2
Internet Explorer 9 STIG Configuration	13

Electionware Clients

Missing Operating System Patches	
Critical	24
Important	51
Moderate	1
Unrated	9

SCAP Misconfigurations	
Windows 7 STIG	51
Firewall STIG Configuration	3
.NET Framework 4 STIG Configuration	2
Internet Explorer 9 STIG Configuration	3
Windows 7 USGCB⁴ Configuration	45
Firewall USGCB Configuration	8

Appendix B: Vendor RFI Analysis: Statewide Voting Machine Contracts

Georgia Vendor RFI Analysis: Statewide Voting Machine Contracts (Millions)							
	ES&S	SOS	OSET	Hart	Smartmatic	Clear Ballot	UNISYN
Total: Hand-Marked Paper Ballots	45.8	247	112	68.5	-	-	63
<i>Total w/ Printing Cost Est (\$28M)*</i>	<i>73.8</i>	<i>247</i>	<i>112</i>	<i>96.5</i>			<i>91</i>
<i>Machines</i>	22.8	60	50	41	-	-	48
<i>Printing, Licensing/Maintenance**</i>	23	187	62	27.5	-	-	15
Caveats	NP	+LM		NP	None	None	NP
Total: Ballot Marking Devices	207.4	207.4	202	174	169	156.5	185.4
<i>Total w/ Printing Cost Est (\$5.8M)*</i>	<i>213.2</i>	<i>213.2</i>	<i>202</i>	<i>179.8</i>	<i>174.8</i>	<i>162.3</i>	<i>191.2</i>
<i>Machines</i>	150	150	131	117	135	101.5	137
<i>Printing, Licensing/Maintenance</i>	57.4	57.4	71	57	34	55	48.4
Caveats	NP	NP		NP	Avg, NP	DNA, NP	NP

*for vendors that did not provide printing cost estimates, OSET Institute's 10 yr estimates were used

**printing, licensing/maintenance costs are over a 10 yr period

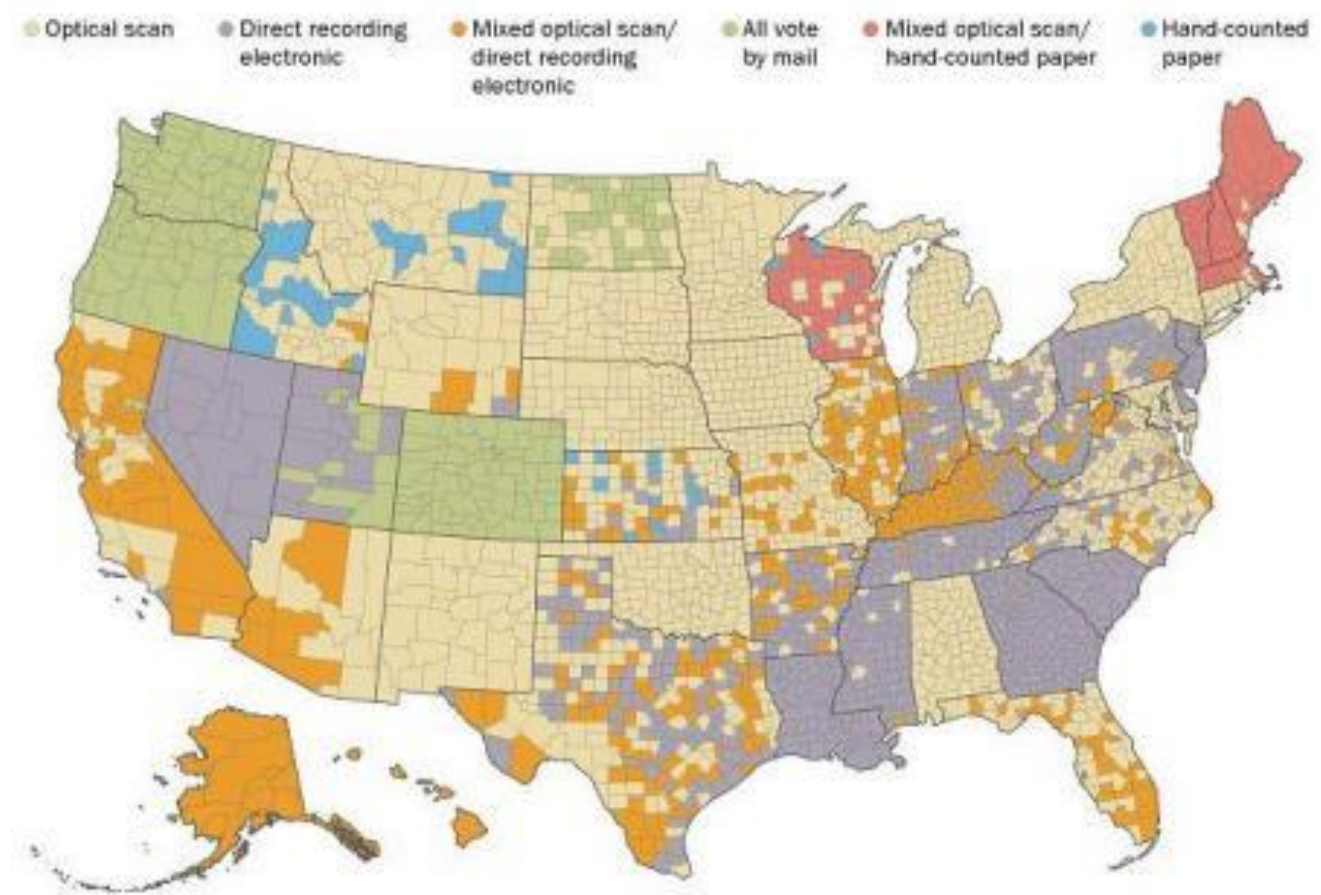
KEY

- **NP:** No printing costs were included in original vendor estimate
- **+LM:** Licensing/maintenance cost added from ES&S report
- **DNA:** Data is not available...unredacted Clear Ballot link broken
- **None:** Did not provide details
- **Avg:** This is the average of the range provided in RFI

Dominion only provided a basic pricing sheet for every voting machine technology they offered. Which machines, how many, additional costs, were time prohibitive details. As such, Dominion was not included.

([GPR](#), 3/13/2019)

Appendix C: Map of Voting Systems Across the U.S.—Pew Research Center/Verified Voting Foundation



([Quartz](#), 7/9/2019)

From: Christina Adkins <CAdkins@sos.texas.gov>
Sent: Tuesday, September 15, 2020 3:41 PM
To: Charles Pinney <CPinney@sos.texas.gov>; 'Parmer, Susan'
>
Cc: >; Keith Ingram <KIngram@sos.texas.gov>
Subject: RE: Texas ExpressVote 1.0 Units

Susan,

This response is very troubling. Essentially, what you've told us over the last couple weeks is that there are Texas customers who received software upgrades that failed the hash validation process, and that although you informed those customers of that fact, you did not inform our office of a known issue with an important procedure on a certified system. This is very concerning and raises doubts about our ability to trust your team to report and address these issues with us.

We also have concerns about the fact that it sounds like your field technicians are the ones who are performing the hash validation process on behalf of the customers. The acceptance testing should be performed by the jurisdiction itself as a way of verifying that the software they have received from the vendor is identical to the version of the system that has been certified by our office. If the hash validation process is performed by the same vendor technician who performed the installation, then that validation process loses one of its major purposes, which is to keep the vendor honest and ensure that the vendor has complied with the certification requirements imposed by the state.

In the short-term, we need a list of all Texas customers who may be potentially affected by this issue. We also need to know if there are any other versions of EVS or other hardware models that have similar issues with the hash validation process, and which customers may be affected by those issues.

In the long-term, we need to have a discussion regarding how this hash validation process will be handled by your Texas customers going forward. This will include additional procedures being provided by our office to those jurisdictions, but going forward with future applications for certification we will also need much more detail from you regarding the instructions and procedures for hash validation that you provide for your customers.

I look forward to your response on those short-term issues. We would like to be able to provide your follow-up response to the examiners so they can consider that response before their reports are submitted in the next few days before their Monday deadline.

090/209

The State of Texas

Elections Division
P.O. Box 12060
Austin, Texas 78711-2060
www.sos.state.tx.us



Phone: 512-463-5650
Fax: 512-475-2811
Dial 7-1-1 For Relay Services
(800) 252-VOTE (8683)

Rolando B. Pablos
Secretary of State

MEMORANDUM

TO: Keith Ingram, Director of Elections, Secretary of State's Office

FROM: Christina Worrell Adkins, Staff Attorney, Elections Division Legal Section

DATE: May 18, 2017

RE: Election System and Software Voting Systems Examination

On April 18-20 2017, Election Systems & Software ("ES&S") presented for examination ES&S EVS 5.4.0.0 voting system. This system includes both components that were previously certified in Texas and new components that had never been through the Texas certification process.

Component Submitted for Certification	Version	Previous Texas Certification
ES&S Voting System (EVS)	5.4.4.0	NA
ElectionWare (and related components)	4.8.0.0	12/15/2016
Election Reporting Manager (ERM)	8.13.1.0	12/15/2016
ExpressVote HW Rev 2.1	2.1.0	N/A
AutoMARK	1.8.7.0	12/15/2016
DS200	2.14.2.0	12/15/2016
DS850	2.11.0	12/15/2016

Pursuant to Texas Administrative Code §81.60, ES&S submitted their application for state certification, Forms 100 and 101, the Technical Data Package, authorization letters, and a copy of all firmware/software and source codes sent directly from NTS, a nationally accredited voting system test laboratory. Examiners were given a copy of the application and testing materials for review prior to the in-person examination that occurred on April 18-20, 2017.

Examination

On Day 1 of the examination, technical examiners, Stephen Berger, James Sneeringer, and I were present to observe and verify the installation of the vendor's software. I was present for observation purposes, but did not participate in the installation portion of the exam. In addition

to observing the installation of the software, the technical examiners also verified version numbers of the software and component parts.

After the installation was completed, I received assistance from Secretary of State Staff Attorney Andre Montgomery with testing the AutoMARK Voter Assist Terminal (“AutoMARK”) and the ExpressVote tabulator terminal for compliance with state and federal accessibility guidelines. The AutoMark was previously certified for use in Texas Elections. The ExpressVote tabulator has never been certified in Texas. However, in 2016, the Secretary of State tested and certified the ExpressVote (without the tabulation features). After reviewing and testing both the AutoMARK and the ExpressVote’s tactile, audio, and visual input devices and approaches to marking and casting a ballot, we determined that both devices met the accessibility guidelines dictated by both federal and state law.

On Day 2 of the examination, all examiners were present. The vendor presented an overview of EVS 5.4.0.0 and provided an explanation and demonstration of the new and existing equipment. The vendor spent a considerable amount of time reviewing the ExpressVote tabulator as this was the only piece of equipment that was new to the Texas certification process. The ExpressVote tabulator has the capability of functioning as both a ballot marking device and a tabulator. This functionality is determined when the programming of the equipment occurs, prior to any ballots being marked or deposited into the tabulator.

Examiners were then given the opportunity to test each piece of equipment with a pre-marked “test deck” of ballots to ensure that the equipment performed the tasks required under state law and accurately tabulated the ballots cast. The pre-marked test deck was marked and hand tallied by staff from the Secretary of State’s office on ballots provided by the vendor. The vendor was not previously made aware of how the ballots would be marked. Some ballots were marked using the AutoMark and ExpressVote before being deposited in the scanners. Voted ballots were tabulated through the DS200 (precinct ballot counter), and DS850 (central tabulator). The tabulation reports from the DS200 and DS850 all matched the hand counted tally from the pre-marked test deck.

On April 20, 2017, ES&S provided an additional demonstration of their online sample ballot program called “ExpressPass.” This program gives the voter the opportunity to call up a sample ballot, make their selections online and print out the pre-marked sample ballot. The sample ballot is printed with both the voter’s selections and a QR code that can be read on the ExpressVote. The sample ballot was not tied to a particular voter, nor were the voter’s on-line selections saved anywhere in the software.

Notable Findings:

1. ExpressVote Tabulator:

Like the previously certified ExpressVote, the ExpressVote tabulator does not require pre-printed ballot stock. A ballot card that is either blank or contains a pre-printed bar code that signifies a particular ballot style is presented to the voter. The voter then starts a voting session by inserting the ballot card into the ExpressVote tabulator. Like the previous certification of the

ExpressVote, the ballot card serves as the ballot of record pursuant to Section 124.062 of the Texas Election Code.

When in tabulator mode, the ExpressVote tabulator not only functions as a ballot marking device; it also contains a scanner that can read the ballot card and record the voter's choice in the same fashion as a traditional precinct scanner. The ballot card would then be deposited into the attached card bin that is locked into a kiosk. The ExpressVote tabulator is not a Direct Record Electronic (DRE) voting machine. When operating in tabulation mode, it is subject to the provisions in the Texas Election Code that pertain to a scanner based voting system. For the ExpressVote tabulator to serve as a precinct scanner, the attached card bin must have sufficient locks and seals in accordance with Section 85.032 of the Texas Election Code. ES&S demonstrated that the card bin could contain two different locks along with seals to prevent unauthorized entry into the card bin. As long as the card bin is secured in a method analogous to a traditional precinct scanner, I believe it could be a viable option for smaller entities and could reduce their election costs as it would combine two pieces of equipment (ballot marking device/precinct scanner) into one. A concern worth noting is that the card bin only has the capacity to hold approximately 300 ballot cards. In order to utilize the ExpressVote tabulator, it would have to be used in a smaller election or the Secretary of State would need to create procedures under Section 85.032(e) of the Texas Election Code to address the transfer of voted ballots from a full card bin.

2. ExpressPass software:

ES&S demonstrated their ExpressPass program which allows voters to generate a voter specific sample ballot online, print out a copy of the voter's potential ballot choices, and use the QR code generated with the online sample ballot to expedite their voting session on an ExpressVote. The ExpressPass does not contain any identifying information related to a voter other printing a map of to the appropriate polling place location for that ballot. The servers do not save any information when generating the ExpressPass nor does using the ExpressPass in the polling place require any connection to the internet. Because this program allows the voters the privacy to make their selections without assistance from an election official and could help to reduce the amount of time voters use each voting station, I believe this feature would be beneficial for use in Texas Elections.

Using the ExpressPass as an online sample ballot generator does not appear to fall under the scope of certification as this is not considered part of the voting system and was not part of the EAC certification. With respect to Texas certification, the only concern with the ExpressPass would be the QR code scanner that the ExpressVote uses to scan the sample ballot and call up the voter's selections. The Secretary of State could place limitations on this part of the product, but any concerns would need to be weighed against the potential benefits to the disability community.

CONCLUSIONS

Over the course of the in-person examination and the review of the materials that were contained in the vendor's application, there was no evidence that EVS 5.4.0.0 along with the DS200, DS800, AutoMARK, and ExpressVote tabulator failed to comply with the Voting System

Standards outlined in Sections 122.001, 122.032, 122.033, and 122.0331 of the Texas Election Code or the rules outlined in Chapter 81, Subchapter C of the Texas Administrative Code.

Overall, EVS 5.4.0.0 met the requirements prescribed by the Texas Election Code, and the Texas Administrative Code that pertain to voting system certification. Therefore, I recommend certification of the aforementioned system.

The State of Texas

Elections Division
P.O. Box 12060
Austin, Texas 78711-2060
www.sos.state.tx.us



Phone: 512-463-5650
Fax: 512-475-2811
Dial 7-1-1 For Relay Services
(800) 252-VOTE (8683)

Rolando B. Pablos
Secretary of State

MEMORANDUM

TO: Keith Ingram, Director of Elections, Secretary of State's Office

FROM: Christina Worrell Adkins, Staff Attorney, Elections Division Legal Section

DATE: May 18, 2017

RE: Election System and Software Voting Systems Examination

On April 18-20 2017, Election Systems & Software ("ES&S") presented for examination ES&S EVS 5.4.0.0 voting system. This system includes both components that were previously certified in Texas and new components that had never been through the Texas certification process.

Component Submitted for Certification	Version	Previous Texas Certification
ES&S Voting System (EVS)	5.4.4.0	NA
ElectionWare (and related components)	4.8.0.0	12/15/2016
Election Reporting Manager (ERM)	8.13.1.0	12/15/2016
ExpressVote HW Rev 2.1	2.1.0	N/A
AutoMARK	1.8.7.0	12/15/2016
DS200	2.14.2.0	12/15/2016
DS850	2.11.0	12/15/2016

Pursuant to Texas Administrative Code §81.60, ES&S submitted their application for state certification, Forms 100 and 101, the Technical Data Package, authorization letters, and a copy of all firmware/software and source codes sent directly from NTS, a nationally accredited voting system test laboratory. Examiners were given a copy of the application and testing materials for review prior to the in-person examination that occurred on April 18-20, 2017.

Examination

On Day 1 of the examination, technical examiners, Stephen Berger, James Sneeringer, and I were present to observe and verify the installation of the vendor's software. I was present for observation purposes, but did not participate in the installation portion of the exam. In addition

to observing the installation of the software, the technical examiners also verified version numbers of the software and component parts.

After the installation was completed, I received assistance from Secretary of State Staff Attorney Andre Montgomery with testing the AutoMARK Voter Assist Terminal (“AutoMARK”) and the ExpressVote tabulator terminal for compliance with state and federal accessibility guidelines. The AutoMark was previously certified for use in Texas Elections. The ExpressVote tabulator has never been certified in Texas. However, in 2016, the Secretary of State tested and certified the ExpressVote (without the tabulation features). After reviewing and testing both the AutoMARK and the ExpressVote’s tactile, audio, and visual input devices and approaches to marking and casting a ballot, we determined that both devices met the accessibility guidelines dictated by both federal and state law.

On Day 2 of the examination, all examiners were present. The vendor presented an overview of EVS 5.4.0.0 and provided an explanation and demonstration of the new and existing equipment. The vendor spent a considerable amount of time reviewing the ExpressVote tabulator as this was the only piece of equipment that was new to the Texas certification process. The ExpressVote tabulator has the capability of functioning as both a ballot marking device and a tabulator. This functionality is determined when the programming of the equipment occurs, prior to any ballots being marked or deposited into the tabulator.

Examiners were then given the opportunity to test each piece of equipment with a pre-marked “test deck” of ballots to ensure that the equipment performed the tasks required under state law and accurately tabulated the ballots cast. The pre-marked test deck was marked and hand tallied by staff from the Secretary of State’s office on ballots provided by the vendor. The vendor was not previously made aware of how the ballots would be marked. Some ballots were marked using the AutoMark and ExpressVote before being deposited in the scanners. Voted ballots were tabulated through the DS200 (precinct ballot counter), and DS850 (central tabulator). The tabulation reports from the DS200 and DS850 all matched the hand counted tally from the pre-marked test deck.

On April 20, 2017, ES&S provided an additional demonstration of their online sample ballot program called “ExpressPass.” This program gives the voter the opportunity to call up a sample ballot, make their selections online and print out the pre-marked sample ballot. The sample ballot is printed with both the voter’s selections and a QR code that can be read on the ExpressVote. The sample ballot was not tied to a particular voter, nor were the voter’s on-line selections saved anywhere in the software.

Notable Findings:

1. ExpressVote Tabulator:

Like the previously certified ExpressVote, the ExpressVote tabulator does not require pre-printed ballot stock. A ballot card that is either blank or contains a pre-printed bar code that signifies a particular ballot style is presented to the voter. The voter then starts a voting session by inserting the ballot card into the ExpressVote tabulator. Like the previous certification of the

ExpressVote, the ballot card serves as the ballot of record pursuant to Section 124.062 of the Texas Election Code.

When in tabulator mode, the ExpressVote tabulator not only functions as a ballot marking device; it also contains a scanner that can read the ballot card and record the voter's choice in the same fashion as a traditional precinct scanner. The ballot card would then be deposited into the attached card bin that is locked into a kiosk. The ExpressVote tabulator is not a Direct Record Electronic (DRE) voting machine. When operating in tabulation mode, it is subject to the provisions in the Texas Election Code that pertain to a scanner based voting system. For the ExpressVote tabulator to serve as a precinct scanner, the attached card bin must have sufficient locks and seals in accordance with Section 85.032 of the Texas Election Code. ES&S demonstrated that the card bin could contain two different locks along with seals to prevent unauthorized entry into the card bin. As long as the card bin is secured in a method analogous to a traditional precinct scanner, I believe it could be a viable option for smaller entities and could reduce their election costs as it would combine two pieces of equipment (ballot marking device/precinct scanner) into one. A concern worth noting is that the card bin only has the capacity to hold approximately 300 ballot cards. In order to utilize the ExpressVote tabulator, it would have to be used in a smaller election or the Secretary of State would need to create procedures under Section 85.032(e) of the Texas Election Code to address the transfer of voted ballots from a full card bin.

2. ExpressPass software:

ES&S demonstrated their ExpressPass program which allows voters to generate a voter specific sample ballot online, print out a copy of the voter's potential ballot choices, and use the QR code generated with the online sample ballot to expedite their voting session on an ExpressVote. The ExpressPass does not contain any identifying information related to a voter other printing a map of to the appropriate polling place location for that ballot. The servers do not save any information when generating the ExpressPass nor does using the ExpressPass in the polling place require any connection to the internet. Because this program allows the voters the privacy to make their selections without assistance from an election official and could help to reduce the amount of time voters use each voting station, I believe this feature would be beneficial for use in Texas Elections.

Using the ExpressPass as an online sample ballot generator does not appear to fall under the scope of certification as this is not considered part of the voting system and was not part of the EAC certification. With respect to Texas certification, the only concern with the ExpressPass would be the QR code scanner that the ExpressVote uses to scan the sample ballot and call up the voter's selections. The Secretary of State could place limitations on this part of the product, but any concerns would need to be weighed against the potential benefits to the disability community.

CONCLUSIONS

Over the course of the in-person examination and the review of the materials that were contained in the vendor's application, there was no evidence that EVS 5.4.0.0 along with the DS200, DS800, AutoMARK, and ExpressVote tabulator failed to comply with the Voting System

Standards outlined in Sections 122.001, 122.032, 122.033, and 122.0331 of the Texas Election Code or the rules outlined in Chapter 81, Subchapter C of the Texas Administrative Code.

Overall, EVS 5.4.0.0 met the requirements prescribed by the Texas Election Code, and the Texas Administrative Code that pertain to voting system certification. Therefore, I recommend certification of the aforementioned system.