EXHIBIT A

DEFCON 25 Voting Machine Hacking Village

Report on Cyber Vulnerabilities in

U.S. Election Equipment, Databases, and Infrastructure

September 2017

Co-authored by:
Matt Blaze, University of Pennsylvania
Jake Braun, University of Chicago & Cambridge Global Advisors
Harri Hursti, Nordic Innovation Labs
Joseph Lorenzo Hall, Center for Democracy & Technology
Margaret MacAlpine, Nordic Innovation Labs
Jeff Moss, DEFCON

Forward

I've spent my entire adult life in the national security arena: Europe during the Cold War, the Balkans in the 1990s, the Middle East since 9/11, in the Pentagon, the White House, and most recently at NATO headquarters in Brussels. I've studied national security at West Point and at Harvard. So, why am I now introducing a report on cyber hacking of our voting systems?

The answer is simple: last year's attack on America's voting process is as serious a threat to our democracy as any I have ever seen in the last 40+ years – potentially more serious than any physical attack on our Nation. Loss of life and damage to property are tragic, but we are resilient and can recover. Losing confidence in the security of our voting process – the fundamental link between the American people and our government – could be much more damaging. In short, this is a serious national security issue that strikes at the core of our democracy.

This report makes one key point: our voting systems are not secure. Why is this so serious? Why must we act now? Why is this a national security issue? First, Russia has demonstrated successfully that they can use cyber tools against the US election process. This is not an academic theory; it is not hypothetical; it is real. This is a proven, credible threat. Russia is not going away. They will learn lessons from 2016 and try again. Also, others are watching. If Russia can attack our election, so can others: Iran, North Korea, ISIS, or even criminal or extremist groups. Time is short: our 2018 and 2020 elections are just around the corner and they are lucrative targets for any cyber opponent. We need a sense of urgency now. Finally, this is a national security issue because other democracies – our key allies and partners – are also vulnerable.

Thousands of state and local election officials are responsible for administering elections but they are often overburdened and under-resourced. It is not their job alone to deal with this national security threat.

This important report highlights the problems that demand our attention and solutions. The "Voting Village" at DEFCON in July 2017 was not intended to be something to entertain hackers. It was intended to make clear how vulnerable we are. The report describes clearly why we must act with a sense of urgency to secure our voting systems.

For over 40 years I voted by mailing an absentee ballot from wherever I was stationed around the world. I assumed voting security was someone else's job; I didn't worry about it. After reading this report, I don't feel that way anymore. Now I am convinced that I must get involved. I hope you will read this report and come to the same conclusion.

Douglas E. Lute
Former U.S. Ambassador to NATO
Lieutenant General, U.S. Army, Retired

Contents

Introduction

Since its founding in 1993, DEFCON has become one of the world's largest, longest-running, and best-known hacker conferences. This year's DEFCON was held July 27-30, 2017 in Las Vegas and drew a record-breaking 25,000 participants. For the first time, DEFCON featured a Voting Machine Hacking Village ("Voting Village") to highlight cyber vulnerabilities in U.S. election infrastructure – including voting machines, voter registration databases, and election office networks. The voting machines available in the Voting Village were paperless electronic voting machines, and at a time when a number of U.S. voting jurisdictions are either committed to or considering purchasing newer equipment based on auditable paper records,[1] open examination of these types of systems could not be timelier. The event was organized by several cyber, voting equipment, and national security experts, along with DEFCON founder Jeff Moss.

The Voting Village acquired and made available to participants over 25 pieces of election equipment including voting machines and electronic poll books. Most models are still widely used in U.S. state and local elections today (with the exception of the AVS WinVote, described below). The Voting Village also featured a mock back-office training "range" to simulate databases and networks of real-world election administrators.

Hacking into voting machines is not new, but previously it was conducted in only in very limited academic or industrial settings under strict controls and publications restrictions. DEFCON's Voting Village represented the first occasion where mainstream hackers were granted unrestricted access to explore and share any discovered vulnerabilities. Legal restrictions including the 1998 Digital Millennium Copyright Act (DMCA)[2] and, to some extent, the Computer Fraud and Abuse Act, made such activities subject to criminal or civil liability.

A consequence of the limited access to voting machine hardware in the past, is that doubts have been frequently raised about if the various vulnerabilities identified in previous studies would be practical for technologists of ordinary skill to discover and exploit. At the DEFCON event, however, thousands of participants were invited to engage with and explore voting equipment and the network simulator in an environment free of restriction for the first time.

The results were sobering. **By the end of the conference, every piece of equipment in the Voting Village was effectively breached in some manner. Participants with little prior knowledge and only limited tools and resources were quite capable of undermining the confidentiality, integrity, and availability of these systems**, including:

- The first voting machine to fall – an AVS WinVote model – was hacked and taken control of remotely in a matter of minutes, using a vulnerability from 2003, meaning that for the entire time this machine was used from 2003-2014 it could be completely controlled remotely, allowing changing votes, observing who voters voted for, and shutting down the system or otherwise incapacitating it.
- That same machine was found to have an unchangeable, universal default password – found with a simple Google search – of "admin" and "abcde."
- An "electronic poll book", the Diebold ExpressPoll 5000, used to check in voters at the polls, was found to have been improperly decommissioned with live voter file data still on the system; this data

[1] Jenni Bergal, "Russian Hacking Fuels Return to Paper Ballots", *Huffington Post Stateline*, (Oct. 3, 2017), http://www.huffingtonpost.com/entry/russian-hacking-fuels-return-to-paper-ballots_us_59d39962e4b092b22a8e398d

[2] U.S. Copyright Office Summary, The Digital Millennium Copyright Act of 1998, December 1998, https://www.copyright.gov/legislation/dmca.pdf

should have been securely removed from the device before reselling or recycling it.[3] The unencrypted file contained the personal information – including home residential addresses, which are very sensitive pieces of information for certain segments of society including judges, law enforcement officers, and domestic violence victims – for 654,517 voters from Shelby County, Tennessee, circa 2008.

Moreover, a closer physical examination of the machines found, as expected, multiple cases of foreign-manufactured internal parts (including hardware developed in China), highlighting the serious possibility of supply chain vulnerabilities. This discovery means that a hacker's point-of-entry into an entire make or model of voting machine could happen well before that voting machine rolls off the production line. With an ability to infiltrate voting infrastructure at any point in the supply chain process, then the ability to synchronize and inflict large-scale damage becomes a real possibility. Also, as expected, many of these systems had extensive use of binary software for subcomponents that could completely control the behavior of the system and information flow, highlighting the need for greater use of trusted computing elements to limit the effect of malicious software. In other words, a nation-state actor with resources, expertise and motive – like Russia – could exploit these supply chain security flaws to plant malware into the parts of every machine, and indeed could breach vast segments of U.S. election infrastructure remotely, all at once.

Given the federal government's recent designation[4] of election systems as critical infrastructure – and in light of what is known about the Russian attempts to infiltrate election networks in at least 21 states in the 2016[5] Presidential Election – it is overwhelmingly evident that election security is now an extension of *national security*. In addition to Russia, other state and private actors (including Iran, North Korea, organized crime, terrorist groups, and even lone-wolf hackers) also possess the technical capability to attack our voting systems or credibly sow distrust in election results. Organized crime is also a serious threat in the larger cybercrime ecosystem and they may also have motives to attack election systems or provide such services for hire, which we've seen in areas like botnets, ransomware, and malware distribution. **The bottom line is: No matter the level of nation-state hacking or interference in 2016, if our enemy's goal is to shake public confidence about the security of the vote, they may already be winning.** And with critical

[3] Michelle De Mooy, Joseph Jerome, and Vijay Kasschau, "The Legal, Policy, and Technical Landscape Around Data Deletion", *Center for Democracy & Technology*, (2017) https://cdt.org/files/2017/02/2017-02-23-Data-Deletion-FNL2.pdf

[4] See Presidential Policy Directive (PPD) 21: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[5] Congressional Testimony of Jeanette Manfra, then-Acting Deputy Under Secretary for Cybersecurity and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security, and Dr. Samuel Liles, Acting Director, Cyber Division, Office of Intelligence and Analysis, U.S. Department of Homeland Security, for a hearing entitled "Russian Interference in the 2016 U.S. Elections," before the Select Committee on Intelligence, United States Senate, on June 21, 2017. Link here: https://www.intelligence.senate.gov/sites/default/files/documents/os-jmanfra-062117.PDF

elections in 2018 and 2020, efforts to hack American democracy will only continue unless safeguards are put in place.

The encouraging news is that a growing, diverse group of stakeholders are embracing election security as national security. As evidenced by the robust, diverse turnout at the Voting Village, understanding cyber threats to our democracy is not just a "hacker thing." Bipartisan stakeholders from federal, state, and local government participated in the Voting Village. Advocacy groups, private sector businesses, think tanks, and national security, intelligence, and military leaders also contributed to the event. The level of interest and support from these groups and individuals parallels an outside movement that views election security as a national security imperative. Many are pressing for policy solutions and practical efforts that leverage best practices already embraced by the cybersecurity community, tailored to the unique nature of elections.[6]

On the Eve of DEFCON: The State of Our Election Security Landscape

For years, computer science and cybersecurity experts have been sounding the alarm on U.S. election infrastructure which can best described as a patchwork of aging, insecure voting systems that vary from state-to-state. As their research has shown, among the most vulnerable voting systems are Direct Recording Electronic (DRE) voting machines. These systems utilize digital touch-screen technology and record votes on the internal memory of the machine, with no paper backup. Cautions about DREs have prompted some changes and a few victories. For example, in 2015 just weeks before a primary election, the State of Virginia decommissioned use of the AVS WinVote (a DRE machine featured at the Voting Village) because of a litany of problems including its Windows operating system, unchangeable default password, the ability to hack the machine remotely, and the fact that its results were transmitted via wireless connections.

There is still more work to be done. Currently there are five states – Delaware, Georgia, Louisiana, New Jersey and South Carolina – that are still operating entirely on paperless systems. Another 9 are partially paperless, making a total of 14 states that are still operating in a highly vulnerable manner.[7] Yet even when leaders recognize change is needed, other competing policy priorities or lack of resources at the state and local level can impede action.

Election security threats grew even more urgent this past election cycle when Government officials confirmed that a foreign adversary, Russia, attempted to interfere in the 2016 United States Presidential Election via "a multi-faceted approach intended to undermine confidence in our democratic process." According to U.S. intelligence official reports, Russia targeted voter registration databases in at least 21 states and sought to infiltrate the networks of voting equipment vendors, political parties, and at least one local election board.[8]

[6] Zetter, Kim. "Virginia Finally Drops America's 'Worst Machine'" *Wired*. August 17, 2015. Link: https://www.wired.com/2015/08/virginia-finally-drops-americas-worst-voting-machines/

[7] Verified Voting, "Voting Equipment in the United States" https://www.verifiedvoting.org/resources/voting-equipment/

[8] Congressional Testimony of Jeanette Manfra, National Protection and Programs Directorate, U.S. Department of Homeland Security, and Dr. Samuel Liles, Acting Director, Cyber Division, Office of Intelligence and Analysis, U.S. Department of Homeland Security, for a hearing entitled

Election administration has always been the constitutional responsibility of state and local jurisdictions. But when Russia – which has also been known to hack elections abroad[9] – decided to meddle in the 2016 U.S. election, it changed the game. The conversation has now been elevated to the level of military and homeland security experts who are increasingly getting involved to help dissect the motives, capabilities and implications of cyberattacks launched at the U.S. and our democracy, as well as assess what kinds of deterrents are available (beyond the scope of this report).

Voting Village Goals

It is through the lens of the complex election security landscape – and on the heels of the Russian 2016 attacks – that Voting Village organizers presented the idea for the village to DEFCON. Media coverage and Congressional testimony on the Russian hacks has helped to advance awareness regarding cyber threats to elections. Yet Voting Village organizers believed there was still much to unpack. Their belief was that the hacker community, if given unfettered access to voting machines and equipment, would be able to enrich the basis of knowledge. As the largest gathering of hackers in the world, DEFCON would also provide the ideal forum to shine the national spotlight on any findings.

To that end, the goals of the DEFCON Voting Village were to:

- Provide examples of working voting systems for security researchers to evaluate, attack, and otherwise study;
- Educate and raise public awareness about the machinery of U.S. democracy, from the machines to how election technology interacts with legal, market, and normative barriers in elections that do not exist in general purpose computing contexts;
- Stimulate a discussion and ideas regarding how security researchers and hackers can help to make our election infrastructure more safe and secure;
- Create a forum to engage with other non-hacker stakeholders, including federal, state, and local policymakers who will be essential to implementing changes and reforms;
- Provide a training opportunity for state and local elections IT staff to learn about their networks and machines in use in this jurisdiction. For many, the village represented the first opportunity for election officials to study and inspect the very machines they are using in their daily operations, yet have not been legally permitted to study previously.

Equipment

The Voting Village organizers procured a variety of voting equipment for examination. A recent DMCA waiver issued by the Library of Congress made it easier for the Voting Village to obtain the hardware for research purposes. Previous such an act was difficult, and in some cases illegal under the DMCA (of course, cyber criminals would not be so constrained by US law). Most of the equipment in the Village was purchased by DEFCON on secondary markets, such as eBay. The machines featured in the Village included:

- AVS WinVote DRE (software version 1.5.4 / hardware version N/A)
- Premier AccuVote TSx DRE (TS unit, model number AV-TSx, firmware 4.7.8)
- ES&S iVotronic DRE (ES&S Code IV 1.24.15.a, hardware revision 1.1)

"Russian Interference in the 2016 U.S. Elections," before the Select Committee on Intelligence, United States Senate, on June 21, 2017. Link: https://www.intelligence.senate.gov/sites/default/files/documents/os-jmanfra-062117.PDF

[9] Koval, Nikolay. "Revolution Hacking." *Cyber war in perspective: Russian aggression against Ukraine* (2015): 55-58. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Koval_06.pdf

- PEB version 1.7c-PEB-S
- Sequoia AVC Edge DRE (version 5.0.24)[10]
- Diebold Express Poll 5000 electronic pollbook (version 2.1.1)[11]

The Voting Village also featured a "cyber range" – a simulator that created a mock virtual "election official's office" and network, built with the guidance and assistance of a large U.S. election jurisdiction staff who ensured quality control and real-world likeness. This range provided a training opportunity for state and local leaders in attendance to better understand the threats to their specific systems and domains, as well as learned best practices to protect their information and networks. The range was operated by CyberBit – a Ft. Meade, Maryland-based cyber training facility that, beyond DEFCON, has provided multiple industry-tailored training services to government and private sector entities.

Limitations

There were significant limitations of the work at the Voting Village, including:

- Participants had no access to source code, operational data or other proprietary information that is not otherwise legally and publicly available. An actual nefarious actor might have little difficulty obtaining these materials.
- The Voting Village provided only a sample of voting technologies. Organizers obtained what they could get their hands on quickly, legally, and affordably. The most recently used system available was the AVS WinVote, which was decertified by the State of Virginia in 2014. A number of other systems, however, are still in use in U.S. elections including the AccuVote-TSx, Sequoia AVC Edge, and ES&S iVotronic.
- The Village had no access to optical scan or DRE systems with a Voter-Verified Paper Audit Trail (VVPAT). These systems, and those involving ballot marking devices, are the most software-independent and auditable systems, and are increasingly popular and heavily used.
- Finally, there was no access to any backend provisioning, counting, or voter registration systems. These kinds of systems are not generally available on the open market. This is especially significant as the evidence from the 2016 election seems to indicate strongly that these types of voting technologies – not voting machines themselves – were the primary target of Russian hacker attacks.

Technical Findings & "Accomplishments"

AVS WinVote

The Advanced Voting Solutions (AVS) WinVote is a DRE voting system that utilizes touch-screen technology to make a voting selection, and then transmits a voter's choice via a wireless local area network (LAN). The AVS WinVote system was the only system in the Village that had been earlier decertified (in Virginia). It was also the most easily compromised. In addition, physical access to the machine proved just as easy of a path to complete compromise.

Carsten Schürmann, a democracy-tech researcher who hails from Denmark, was able to hack into the AVS WinVote within minutes remotely over Wi-Fi. The WinVote broadcasts its own Wi-Fi access point to which modern operating systems can easily connect. Using commonly available network tools (e.g., Wireshark)

[10] "PEB" stands for Personal Electronic Ballot, which functions similarly to a portable memory pack. It is used to authorize a new voting session by poll-workers and, when the polls close, poll workers move summary data from each machine onto the PEB. The PEBs are then transported to election headquarters or their contents transmitted via a computer network.

[11] An Electronic Pollbook is a system that essentially replaces the spiral-bound lists of registered voters in every polling place by putting that functionality into a laptop, tablet, or kiosk-like computing platform.

Schürmann determined immediately that the WinVote had a specific IP address and was able to use a vulnerability from 2003 (CVE-2003-0352[12]) and preinstalled attack payloads in Metasploit (a vulnerability analysis and penetration testing tool) to gain access to the filesystem and escalate privileges to an admin user – meaning he could make the machine think he was an administrator of the system, not simply a mere voter or poll-worker. Once he had this access, Schürmann was able to do anything on the system, from running code, to changing votes in the database, to turning the machine off remotely. This vulnerability had clearly been in the system since 2003, allowing anyone within 150-300 feet of a polling place complete control of any WinVote machine while it was being used. For $50, a hand-held high gain antenna could be purchased that would extend that range to over 1,000 feet and through walls.

Physical access to the machine afforded similar ease-of-access. The locked panel on the front of the device was easily picked or opened with readily available keys that could be purchased easily and cheaply online. The locked cover was easily bypassed without paying attention to the lock as well (by simply compromising the plastic hinge). The physical security protecting the USB port was ineffective and also irrelevant, due to the findings in the next paragraph.

While examining the case further, DEFCON hackers noticed that there were 2 unprotected, uncovered USB ports on the back of the machine. These were within easy reach of a voter, and unfortunately the privacy screen for the AVS WinVote is so private that it would be difficult to tell if someone was tampering with USB ports on the back of the machine while voting. There was no USB keyboard around in the Voting Village – a natural place to start with an unprotected USB port – but after an errand to a local electronics supply store to obtain one, all hackers had to do was to simply attach the keyboard, type "`ctrl-alt-del`" and the Windows task manager would pop up. At that point, they could type "`alt-f run`" and run any software they wanted to, including software on a USB stick that is inserted into the other USB slot on the back of the machine. As one hacker, Nick, remarked, "With physical access to back of the machine for 15 seconds, an attacker can do anything."

AccuVote-TSx

The AccuVote-TSx is touch screen DRE voting machine, manufactured by Premier/Diebold, that records votes on internal flash memory. In much the same way that an ATM works, voters insert a card into the machine and then pick their choice on a touchscreen. Votes are then recorded to internal electronic computer storage.[13]

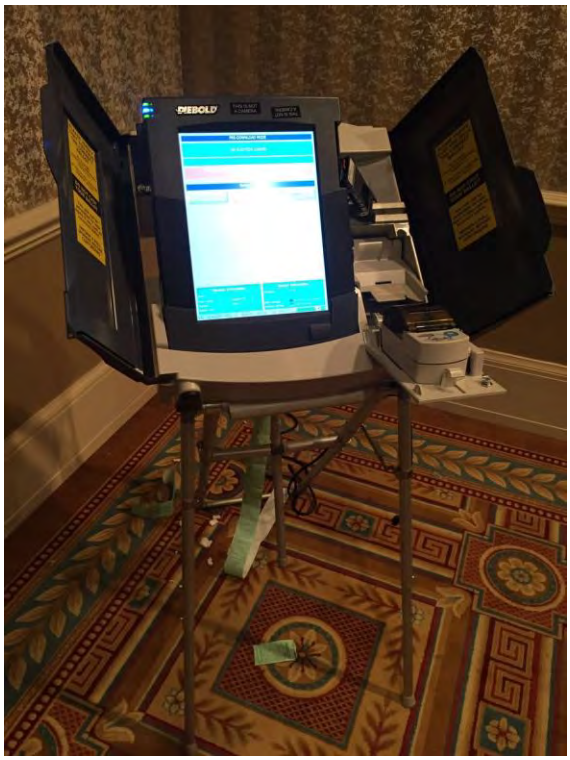
As is natural in any DEFCON Village structured around hardware artifacts, Voting Village hackers seemed to spend more time on platforms other than the AccuVote-TSx. Just as with the ES&S iVotronic below, much of

[12] See: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=can-2003-0352

[13] Verified Voting, "Premier/Diebold (Dominion) AccuVote TS & TSx" https://www.verifiedvoting.org/resources/voting-equipment/premier-diebold/accuvote-tsx/

the work around this machine focused on examining the details of the internal hardware layout and examining the "firmware" – software that runs the low-level hardware functions and is not changed as often as the voting software itself.

Joe Fitzpatrick, Schuyler St. Leger, Ryan (@rqu45 on Twitter), Wasabi, and Ayushman were all involved in examining the innards of the TSx. First, Wasabi noticed that a particular chip (an EPROM chip) was wired to the machines battery controller, and removing this chip caused the machine to be completely inoperable. If not protected carefully, removing such chips from TSx machines could be used to selectively shut down voting in certain areas (assuming physical access and time necessary to open the case of the machine undetectably, remove the chip, and put the machine back together). This chip was socketed rather than soldered in place, making removal quite easy.



Wasabi also noticed that the `NK.bin` file (the main executable or "kernel" for the Windows CE operating system) had local networking and modem support, which would ideally be removed for software in jurisdictions that do not use those functions. Similarly, Ayushman noticed that there was a `.ini` configuration file that seemed to have passwords, users, and the modem configuration for the device, which he suspected could be changed (since there is little access control) with a serial (DB9) connection to the device. After the conference it was confirmed that connecting the debug jumped on the PCB would still activate the boot loader console on the DB9 VIBS.

Fitzpatrick, St. Leger, and Ryan focused on analyzing the firmware of the device and mapping the pins on the chips to functions useful for chip debugging tools. The TSx has what is called a JTAG interface which is a plug on the circuit board typically used during the manufacturing process to check correct functionality. However, after the unit is sold, the JTAG interface is still available and provides convenient access to the processor and the rest of the system. They noticed the TSx processor is an ARMv5 chip and common chip debuggers only go back as far as ARMv6. Therefore, they had to locate an older debugger in order to map the functionality of each pin and interact with the software. There are further details about this work available in the raw notes from the Voting Village on github.[14]

ES&S iVotronic

Like other DRE machines, the iVotronic, manufactured by ES&S, features a touch-screen interface and records votes in internal memory. A poll worker uses a device called a PEB (roughly the size of a deck of playing cards) to enable voting for each voter. PEBs are also used to store and aggregate the final vote tallies from all machines that are then physically transported to election headquarters. In some configurations, the PEB tally can be alternatively transmitted to headquarters over a computer network.[15]

[14] See: https://github.com/josephlhall/dc25-votingvillage-report/blob/master/notes-from-folks-redact.md#premier-accuvote-tsx

[15] Verified Voting, "Election Systems and Software (ES&S) iVotronic" https://www.verifiedvoting.org/resources/voting-equipment/ess/ivotronic/

Similar to the AccuVote-TSx, many of the interesting findings about the iVotronic related to examining the internals of the various components. Hackers in the Village examined the PEB device, the PEB readers, and the iVotronic DRE machine.

A hacker named Scott Brion examined the PEB and PEB reader. He found the PEB contains an 8-bit processor, EPROM (non-volatile storage, not easy to update), flash memory (non-volatile storage, easy to update), an infrared communications port (IRdA), a magnet, serial pins and a battery. The PEB reader – a device that serves as an interface for reading PEBs one by one to transfer contents – contained similar elements, including an 8-bit processor, EPROM, USB port, serial pins, and an IRdA receiver port. Brion was able to establish communication to the firmware through the serial PINs, however nothing of value was obtained (in some cases "security fuses" may have been intentionally blown by the manufacturer to prevent analysis and readout of firmware). With a bit of research, it became clear that green PEBs were "supervisor" units used to start and end elections on a set of machines and the security fuses are blown on those, preventing analysis and extraction of firmware on those units. However, the red PEBs, used to accumulate election data and authorize each new voter to vote did not have their security fuses blown, so the firmware analysis proceeded on those units. This is likely an inferior security design as the red PEBs actually accumulate and transmit vote totals, which is exactly what an attacker seeking to change an election result would attack by changing the firmware in a PEB or swapping a PEB out with a clandestine attacker PEB.

Another Village participant, Kris Hardy, also focused on attacking the PEBs and PEB readers as possible ways to get into the iVotronic in a way that could be undetectable (and mimic the goals of a malicious election attacker). Hardy and his colleagues (who asked not to be identified) used a PICkit 3 chip debugger/programmer and were able to identify several PEB chips that were configured without their security fuses blown (meaning the chips could be easily analyzed and interacted with). They were able to extract firmware from one of the chips, which they were able to decompile (a process that turns binary computer code into source code that humans can read – the opposite of "compiling" source code software into a binary executable). The contents looked promising but they did not have time to fully examine the firmware before the Village had to close. They recorded the chip pin-outs (mapping the pins to functionality on a debugger/programmer) in an online github repository for future researchers.[16]

Sequoia AVC Edge

The Sequoia AVC Edge, a Dominion product, is another widely-used DRE machine where voters insert a "smart-card" into the machine (a credit card-sized card that authorizes a voter to vote), pick their voting choice on a touchscreen, and then the results are recorded on the machine's internal storage. When polls close, the votes for a particular machine are written to a "PCMCIA" flash memory card which is removed from the system and either physically transported to election headquarters or their contents transmitted via computer network.[17]

[16] See: https://github.com/josephlhall/dc25-votingvillage-report/blob/master/notes-from-folks-redact.md#ess-ivotronic

[17] Verified Voting, "Sequoia (Dominion) AVC Edge" https://www.verifiedvoting.org/resources/voting-equipment/sequoia/avc-edge/

Note: As is the case with opportunistic hacking projects like the Voting Village, some equipment will receive more attention than others; in this case, the Sequoia AVC Edge did not attract as much attention as other systems. Below, we describe what are less findings and more features of what hackers found remarkable about this system.

Members of the University of Houston Cybersecurity Club – Tsukinaki and Joe (no last names given) – spent some time with the Sequoia AVC Edge. Through their investigation, it was determined that the AVC Edge has an internal CompactFlash (CF) card running on the pSOS operating system, a real-time operating system developed in 1989, before many of the Voting Village participants were born. This particular operating system has traditionally been used heavily in retail and kiosk equipment.

The Houston team also found that the Edge records data as a hex file; meaning it was difficult to figure out what the contents were without a bit more additional information or reverse-engineering of the file format (a labor-intensive activity not well-suited for the Village). Voting results were stored on the CF card, but then also sent to flash storage on a PCMCIA card in a slot in the back of the machine. It was obvious from the data that this particular AVC Edge was from the 24th precinct of Washington DC, which hackers got by just running the command strings on the data. In this process, one could definitely see the slate of candidates and such, though no voter identities or similar personal voter data was viable. (This was expected as no voter identity could make it from the pollbook process to the voting machine).

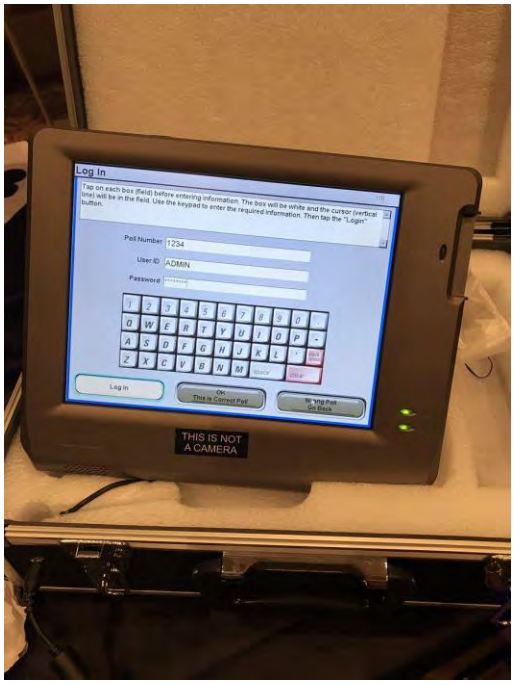
Hackers then tried to boot the operating system image in a virtual machine, but did not get too far; One could see a menu in the PSOS boot file – that is, could see the strings, but could not get it to boot. There was a RAM file that seemed to give them a "file not found" in the boot sequence. Nick used a utility called `binwalk` – a firmware reverse-engineering and analysis tool – to examine the firmware and it appeared that there may be use of an *8-bit cipher* (eight (8) bits is exceedingly insecure).

Diebold ExpressPoll 5000

While the devices detailed above are types of vote-recording and vote-casting equipment, the Village also had available an electronic pollbook (the ExpressPoll 5000), which is still currently used in states like Ohio to check in voters on Election Day. At the Voting Village, the pollbook was subject to a significant degree of scrutiny by participants, including:

Voter Data Leakage

On day 1 in the Voting Village, it was discovered that the ExpressPoll units obtained were not properly decommissioned and still contained voter records. Specifically, 650k voter records from Shelby County, Tennessee were still present on the pollbooks, containing names, addresses, dates of birth, driver's license numbers and a number of other potentially sensitive fields. Village organizers secured the data, removed it from the units available in the village, and one village organizer began a process of disclosure to Shelby County so that they could be aware of the issue.



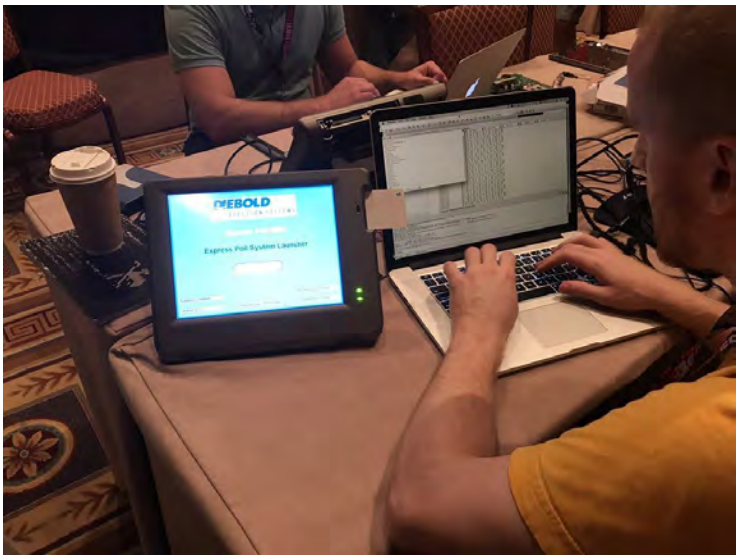
Technical Findings

The unit did not have much in the way of physical security protections, allowing someone with a screwdriver to remove and replace the election media, or simply remove it to accomplish a denial-of-service attack. The default username and password for this unit was available with a simple google search. There were also two USB ports that seemed unprotected.

The ExpressPoll runs on an obsolete embedded operating system, Windows CE 5, and validates no input or software updates (it would load without any prompting or checking both a new bootloader – commands that tell the system how to start up – and OS image – the operating system the device runs after start-up). This could allow attackers to inject a new bootloader (which appears to be proprietary) or Windows CE image without detection. Similarly, the unit reads a file "`ExPoll.resources`" that contains all the parameters for the election that could also be injected with parameters chosen by an attacker. When the pollbook software is launched, this file is loaded into memory and then saved to non-volatile storage for use in future elections. Village hackers were able to change the parameters in this file, get it to load and have their own parameters loaded (in this case they "bricked" – rendered inoperable – an ExpressPoll unit, but were confident that further testing would have resulted in successful modification of pollbook parameters).

Hackers attempted to crash the main application by loading large amounts of data into the database fields, but this only slowed the device, instead of crashing the main application and potentially allowing further access. The unit's networking seemed to be well-locked down with essentially only data being broadcast from the unit and hackers were unable to make a successful connection and inject data through the network interface.

There was some hope that changing the `Consolidation_ID` on a smartcard that the unit writes to in order to authorize a voter would have silently discarded that voter's vote, but that was not possible to test without a smart card reader/writer, which was unavailable.



The device keeps an event log with login, logout, power, load, and open events. However, this log would not be sufficient to prevent tampering; it is only written by the device and does not reflect any file changes that occur on the storage media (and, of course, is not integrity protected).

Impact & Lessons Learned

The technical findings of the Voting Village were not entirely new. As stated, hackers and researchers have breached these voting machines before under various circumstances. However, this experiment allowed mainstream hackers more time and access than ever before, generating several "real-world" lessons that policymakers should consider moving forward:

Lesson #1: Even with limited resources, time, and information, voting systems can be hacked.
The DEFCON Voting Village showed that technical minds with little or no previous knowledge about voting machines, without even being provided proper documentation or tools, can still learn how to hack the machines within tens of minutes or a few hours. Past official studies such as the California Top-To-Bottom Review[18] and the Ohio EVEREST Review,[19] conducted over ten years ago had significant restrictions on what participating researchers were allowed to try. Those studies were also done in a "white box" environment where researchers had access to source code, documentation, and equipment under strict non-disclosure agreement.

In the case of the DEFCON Voting Village, hackers had to create, copy, or cobble together their own tools though, in turn, they were given permission to fully experiment and take risks that may result in the machines being destroyed in the process.

The good news is, freedom to take such risks accelerates the process and can lead to completely new discoveries of new vulnerabilities. The bad news is, if relative rookies can penetrate a machine or system in a matter of hours, it becomes incredibly difficult to deny that a skilled, nefarious hacker – including sophisticated cyber criminals or nation-state attackers – with unlimited time and resources, could not do the same.

Lesson #2: Foreign-made parts introduce serious supply chain concerns.
"Phishing" scams via email are common, and for good reason: When successful, phishing can provide inside access to a machine, account, system or network without the hacker actually having physical access to the machine. Information can then be stolen or exploited in some fashion, without the victim ever knowing that entry has occurred. U.S. intelligence reports reveal that Russians were not only interested in hacking into voter databases but also into other aspects of the election, including the software supply chain. According to that report, Russian hackers affiliated with Russian military intelligence – the GRU – sent phishing emails to employees at a voting services company that provides state and local election offices with voter registration systems, comprising at least one account on that vendor's system that was then used to send spear-phishing emails to 120 local and state election officials.[20] Given the typical successes of a well-designed spear-phishing attack, we can be almost certain that one or more election officials fell victim to this attack, although we do not know what access and damage might have resulted (as this information is likely still classified).

Good cyber hygiene can help prevent some of these remote attacks. However, during the Voting Village, the extensive use of foreign-made computer parts – frankly, as expected given how many commercial computing devices are manufactured overseas – within the machines opened up a serious set of concerns that are very relevant in other areas of national security and critical infrastructure: the ability of malicious actors to hack our democracy remotely, and well before it could be detected. A frequent argument raised about the

[18] See: http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/

[19] See: https://www.eac.gov/assets/1/28/EVEREST.pdf

[20] National Security Agency, "Report on Russian Spear-Phishing" November 2016. Parts redacted.
https://assets.documentcloud.org/documents/3766950/NSA-Report-on-Russia-Spearphishing.pdf

defensibility of election systems is that the diversified, decentralized nature of our election infrastructure provides at least some protection from wide-scale hacks. But via a supply chain originating overseas, voting equipment and software can be compromised at the earliest of stages in manufacturing process. For example, foreign actors could design or plant a virus in software, memory, or even a small microchip that could affect an entire make/model of voting machine, theoretically allowing them to be compromised in one coordinated attack. To be sure, while we've known for over a decade that some voting machines have hardware manufacturing and/or assembly in foreign countries, less is known about sourcing of software. We do know, for example, of one case when Election Systems & Software failed to disclose it was manufacturing products in a sweatshop in the Philippines in 2007.[21]

One additional implication of foreign parts includes inability to limit insider threats. Cyberattacks originating from inside an organization are a serious concern. Yet U.S. election officials, vendors, or those involved in the voting administration process can be vetted to some degree. This is not the case when the process involves foreign components and facilities, including complicated but common relationships such as subcontractors further subcontracting work out to other entities. To be sure, there are very few entities – the Department of Defense, the National Security Agency, and large tech companies such as Google and Facebook – that have the ability and resources to design, develop, and manufacture entire computer systems on their own; a controlled supply-chain is a first step towards reducing these kinds of threats, but it would be best if voting systems moved to more trusted system design.

Lesson #3: This was more than a "hacker" stunt and showed that a diverse community of stakeholders must be engaged.

Organizers did not maintain a precise count of how many entered the Voting Village but estimate that the number exceeded several thousand. In just three days, the Voting Village expanded the number of people who have now had first-hand experience and knowledge of these systems. By Sunday, the attendees who started hacking on Friday had become the experts and they were teaching and helping the new people who just started on Sunday. Exponentially expanding the knowledge base in this regard is sure to have great impact on the solutions and policy-making process. Remarkably, many of the hackers that stayed in the Voting Village for a considerable amount of time at DEFCON 25 were young, between the ages of 16-19, demonstrating to organizers that this kind of civic infrastructure hacking may be a promising way to reach out to younger elements of the information security community.

Additionally, given the wide scope of stakeholders involved in election security, Voting Village organizers believed it was essential the Village did not come to be seen only as a "hacker thing." Organizers reached out to and involved hundreds of other "non-hackers" in the event, ranging from senior leaders of NGOs, to cyber and voting experts, to elected officials to national security leaders. Staff from U.S. Senate Homeland Security & Governmental Affairs Committee and representatives from National Institute for Standards & Technology (NIST), the U.S. Department of Homeland Security (DHS) and the National Governors Association (NGA) attended.[22] Members of the U.S. Congressional Cyber Caucus including Representative Will Hurd (R-TX) and Representative Jim Langevin (D-CT) also visited the Voting Village.

The Voting Village also intentionally encouraged state and local election officials to attend. For many of them in attendance, the Village was their first opportunity to look themselves into the machines – machines they are required to use and manage, but have been prohibited to study in depth – and find answers to their own

[21] Kim Zetter, "ES&S Failed to Disclose Manila Manufacturer to Fed Agency," *WIRED News*, August 14, 2007. https://www.wired.com/2007/08/ess-failed-to-d/

[22] APPENDIX #1: Partial List of Attending Individuals & Organizations

questions and learn more about that equipment. Moving forward, it will be critical to incorporate all of these stakeholders into the security and solutions discussion.

Lesson #4: The Village challenged major criticisms – and reiterated the need for policy change.
Finally, the Voting Village helped to dispel a few long-circulating criticisms – as well as helped to affirm what election security advocates have been arguing for years: There is urgent need for federal, state and local election officials to implement measures to secure U.S. election infrastructure.

First, though voting machine manufacturers have historically denied claims that their machines are insecure, some have suggested the Voting Village demonstration did not constitute a "true" test because it was not conducted in a real election setting. Yet, enemy hackers are certainly not operating in a "sanctioned" environment and if a voting machine can be hacked by a relative novice in a matter of minutes at DEFCON, imagine what a savvy and well-resourced adversary could do with months or years.

Second, there is a common misconception that the internet is required for voting machines to be hacked. Obviously, the WinVote hacked at DEFCON is particularly vulnerable because it creates a local network that is completely unprotected. But even for the machines in the Village (or real world) that do not, they are still not as distant from the internet as it may seem, and many contain software and hardware that can be used to connect them to the internet. Before each election, the ballots need to be created via a software application, which runs on a desktop computer or is web-based. From there, the formatted ballot is transferred and uploaded to voting machines through memory cards or USB sticks. And even well before election day – indeed before a voting machine is assembled, sold to a government, and brought online for an election – the foreign parts in the machines suggest multiple voting systems could be compromised by laying the seeds of future attacks in supply chain processes. This new revelation heightens concerns, and more must be done to protect our systems at every point in the process, including across the supply chain.

Finally, another common argument is that voting systems are insulated to a degree by the diversity and decentralized nature of our election infrastructure. It is true voting systems do vary greatly from state to state, making it difficult to penetrate multiple voting machines simultaneously. Yet, the confirmation of foreign-made parts and software raises the possibility that hackers could take remote control of at least an entire line of voting machines at a later point, with the right level of access in the supply chain. And as pointed out, machines also touch the internet and non-networked forms of data transmission (USB sticks, etc.) at various other points in the process, potentially weakening resilience if not done very carefully. Yet even if that did not happen, the Voting Village helped to show that simply manipulating a voter file (or in the Village's case, poll book data) could create enough problems or long lines to affect an election outcome.

Next Year's Voting Village: Moving Forward

The Voting Village will return to DEFCON in 2018. Organizers hope to expand the event next year to potentially cover a number of distinct areas in addition to hands-on hacking of voting equipment, including:

- **Closed-Loop System:** We would like to have a closed-loop system on which we can run an entire mock election using actual voting technologies. This would include voter registration, ballot generation, a mock polling place (with rules of engagement), and results reporting. This addition would allow us to go a step beyond just looking at the machinery of democracy on the technology level.

- **Election Tech Range:** Election officials and voting system manufacturers have some of their own

security technologies, compositions, or solutions that they find work well in defending against certain threats. We would like to invite election officials and voting system vendors to come and get advice and even testing of their tech. A good example would be if an election official or manufacturer would like to get feedback on a particular security system or challenge security researchers to evaluate it and give feedback on how it could be improved.

- **Election Tech Challenges:** There are a number of activities in elections that are difficult to secure. Some small fraction of votes are cast by email, fax, and web and a larger fraction cast on paper through vote-by-mail. We would like to set up examples of these technologies and challenge Voting Village attendees to demonstrate what failures can happen and to what extent those can be avoided.

- **Election Technology Usable Security Evaluations**: A secure voting system can still be highly usable. We would like to invite usable security researchers to join the village to build up a resource of usability and needs assessment conclusions and profiles of past, existing, and future voting technologies.

- **Request for Donation of Machines, Software, Databases, etc.**: DEFCON has embraced the notion that the DEFCON hacker community's role in the election security debate is one of providing a public service. To that end, DEFCON is offering to test any clerk or secretary of state's election administration equipment and provide training for their IT staff at DEFCON 26. Our door is always open to those who want to make their voting process more secure.

Conclusion

DEFCON organizers believe the Voting Village was vital to growing the base of knowledge, expanding the circle of stakeholders beyond hackers, and shining a national spotlight on the serious cybersecurity weaknesses of U.S. election infrastructure.

The next step is to make clear that this is a conversation that cannot "stay in Vegas." It is imperative that leaders at the federal, state and local level come to understand this threat as a national security imperative and work together – leveraging the support of the national security and cybersecurity community – to better defend and protect the vote from cyberattacks in the upcoming elections in 2018 and 2020. Americans need the reassurance that their democracy is safe, starting at the ballot box.

Acknowledgements

A number of individuals and organizations contributed to the Voting Village and to this report. A special thanks to:

- Organizers, subject-matter-experts and other visionaries who turned the Voting Village concept into a reality and helped to author this report, including especially Sandy Clark.
- ISP/CyberBit and the Cook County, Illinois Clerk's Office for supporting the cyber back-office simulator at the Voting Village;
- Speakers who contributed to the Voting Village discussions including representatives from the Center for Democracy and Technology, Center for Election Integrity, the Center for Internet Security, the National Governors Association, the U.S. National Institute for Standards and Technology (NIST), and Verified Voting.

APPENDIX #1: Partial List of Attending Individuals & Organizations

Representatives attended the event from a variety of organizations including:

- Atlantic Council
- Aries Security
- Cisco
- Center for Internet Security
- Election Assistance Commission (EAC)
- IBM
- McAfee
- Microsoft
- Multi-State Information Sharing & Analysis Center (MS-ISAC)
- National Institute for Standards & Technology (NIST)
- National Governors Association (NGA)
- Nordic Innovation Labs
- Rochester Institute of Technology
- University of Buffalo
- University of Pennsylvania
- University of Texas San Antonio
- US-Computer Emergency Readiness Team (US-CERT)
- U.S. Department of Homeland Security (DHS)
- U.S. Senate Homeland Security & Governmental Affairs Committee
- U.S. Representative Will Hurd, Congressional Cyber Caucus (R-TX)
- U.S. Representative Jim Langevin, Congressional Cyber Caucus (D-CT)
- Verified Voting

EXHIBIT B

DEF CON 26 Voting Village

Report on Cyber Vulnerabilities in

U.S. Election Equipment, Databases, and Infrastructure

September 2018

Co-authored by:
Matt Blaze, University of Pennsylvania
Jake Braun, University of Chicago
Harri Hursti, Nordic Innovation Labs
David Jefferson, Verified Voting
Margaret MacAlpine, Nordic Innovation Labs
Jeff Moss, DEF CON

Contents

Introduction - "Election officials have plenty to learn from hackers"

By: Alex Padilla, Secretary of State, California
Originally published: *The Hill,* August 19, 2018[1]
(reproduced with permission of the author)

Every year, DEFCON convenes thousands of hackers who attempt to breach the security of important technologies in an effort to expose vulnerabilities. For the past two years, this has included voting machines in a room dubbed the "Voting Village."

Rather than watch from the sidelines, or read about the findings in the news, I wanted to see for myself. So, I went to DEFCON. I listened, I observed and I had the opportunity to address attendees.

While it's important to constantly search for and understand the vulnerabilities of any voting system, a unifying message at the conference — from hackers to elections officials alike — is that we must be on alert and Congress must invest more to better secure our elections.

Threats to the integrity of our elections are constantly evolving. Not too long ago, a primary focus for election officials was securing voting machines. Today, cyber attack vectors have expanded — and so must our defenses.

This includes protecting our state voter registration databases, county election management systems, election night reporting websites, state and local government social media accounts and ensuring the information voters consume is accurate.

Intelligence officials tell us that the "warning lights are blinking red" — and our adversaries are getting more sophisticated. It's clear to me, as California's chief elections official, that we cannot become complacent.

That's why attending DEFCON was important. Though, as my secretary of State colleagues are right to point out, the environment under which voting machines were "hacked" at DEFCON do not precisely reflect real-world conditions.

On Election Day, voting machines aren't left on tables to be opened or exposed for hours on end, and there isn't unlimited public access to equipment at polling places or county offices.

Still, we could learn a lot from friendly hackers. Their insight can help us stay one step ahead of those who seek to undermine our democracy. It forces us to take second, third and fourth looks at systems. Elections officials must constantly scrutinize, test, adapt and upgrade security measures.

But no matter how much we learn or how much we innovate, we cannot succeed without adequate resources. Election administrations in America has been historically underfunded and understaffed. The burden of funding for election administration typically falls on the limited budgets of local governments.

[1] Padilla, Alex. "Election Officials Have Plenty to Learn from Hackers." The Hill. August 21, 2018. Accessed September 25, 2018. https://thehill.com/opinion/cybersecurity/402458-election-officials-have-plenty-to-learn-from-hackers.

States have a responsibility when it comes to properly funding election administration, including security. I'm proud that in California we secured $134 million in this year's budget to upgrade or replace voting systems plus additional funding for the creation of the offices of Election Cybersecurity and Enterprise Risk Management.

We're also updating hardware and software, monitoring our networks around the clock, and we've strengthened communications and information-sharing channels with federal authorities.

Still, we can and must do better.

You may have heard that Congress recently appropriated $380 million for election security nationwide. Not quite. Remember butterfly ballots and hanging chads? The recent federal appropriation was simply the final disbursement of money originally approved in 2003 to address the debacle of the 2000 presidential election in Florida.

There has been no new additional funding authorized to address our modern security challenges. To make matters worse, this month, the Republican majorities in both the House and the Senate defeated measures that would have appropriated $250 million for election security grants to states.

Meanwhile, they approved a $700-plus billion national defense appropriation — with not one cent for shoring up our nation's election systems.

Protecting our elections from foreign interference is a matter of national security. That's why our election infrastructure has been designated as critical infrastructure by the Department of Homeland Security.

For elections officials to implement needed election security measures, state and local governments need ongoing funding from federal and state budgets. We can't let up, and we can't rely on dated equipment. The stakes for our democracy are too high.

Until Congress takes our requests seriously and makes the necessary investments to further fortify our voting equipment and systems, election officials must think and act outside the box.

While I'm told I was the first secretary of state to attend DEFCON, I'm confident I won't be the last. We have a responsibility to learn from hackers, particularly those wanting to help. We owe it to the nation to do all we can to protect our elections.

Nothing short of our democracy is at stake.

New Findings on the Eve of the 2018 Midterm Elections

Back for its second year at DEF CON, the world's largest and best-known hacker conference, the Voting Machine Hacking Village (Voting Village) dramatically expanded its hands-on activities and audience in advance of the 2018 midterm elections. When the Voting Village first launched in 2017 - and was attended by thousands of white hat hackers, government leaders, and media - it aimed to identify vulnerabilities within the U.S. election infrastructure. In 2017, intelligence about Russian adversaries hacking the 2016 presidential election was increasing but the severity of the threat to U.S. election infrastructure was dying down. This year, DEF CON dramatically expanded its inquiries to include more of the election environment, from voter registration records to election night reporting and many more of the humans and machines in the middle. DEF CON had a greater variety of voting machines, election officials, equipment, election system processes, and election night reporting. Voting Village participants consisted of hackers, IT and security professionals, journalists, lawyers, academics, and local, state and federal government leaders.

This year, the Voting Village made more than 30 pieces of voting machines and other equipment available to its participants. All of the equipment (with the exception of the AVS WINVote, described below) is still used throughout the United States today. The Voting Village is the only public forum in United States at which hackers have nearly unrestricted access to discover vulnerabilities in the equipment. In addition, this year the Voting Village conducted unprecedented outreach to state and local election officials, inviting them to participate in the Village's activities and receive free training from cybersecurity experts.

As was the case last year, the number and severity of vulnerabilities discovered on voting equipment still used throughout the United States today was staggering. Among the dozens of vulnerabilities found in the voting equipment tested at DEF CON, all of which (aside from the WINVote) are used in the United States today, the Voting Village found:

- A voting tabulator that is currently used in 23 states is vulnerable to be remotely hacked via a network attack. Because the device in question is a high-speed unit designed to process a high volume of ballots for an entire county, **hacking just one of these machines could enable an attacker to flip the Electoral College and determine the outcome of a presidential election**.

- A second critical **vulnerability in the same machine was disclosed to the vendor a decade ago**, yet that machine, which was used into 2016, still contains the flaw.

- Another machine used in 18 states was able to be hacked in only two minutes, while it takes the average voter six minutes to vote. **This indicates one could realistically hack a voting machine in the polling place on Election Day within the time it takes to vote.**

- Hackers had the ability to **wirelessly reprogram, via mobile phone, a type of electronic card used by millions of Americans to activate the voting terminal to cast their ballots**. This vulnerability could be exploited to take over the voting machine on which they vote and cast as many votes as the voter wanted.

Further, in partnership with two other DEF CON villages, including r00tz Asylum, which allows children (accompanied by an adult) to learn and test white hat techniques, and Capture the Packet (CTP), the most popular competition at DEF CON, young DEF CON attendees were given the opportunity to hack mock ups of secretary of state election results websites for the thirteen Presidential Battleground States. In less than

10 minutes, an 11-year old in the competition hacked into a mock up of Florida's election results website, changing its reported vote totals. The attack the children were trained to use on the sites (SQL injection) is the same attack the Senate Intelligence Committee warned was used in a majority of Russian cyber attacks on election websites in 2016.[2] Further, the Open Web Application Security Project (OWASP), one of the leading organizations on website security globally, has cited this type of attack as the top web application security risk for organizations around the world.[3] While children in the r00tz Asylum village used this vulnerability for a variation of 'de-facing,' which is generally considered to be an easily found, "show-off" attack, in the hands of more skilled and malicious adversaries the underlying vulnerability can be used to initiate much more serious types of attacks.

Aside from introducing the youngest members of the DEF CON community to issues related to civics, media, and cybersecurity, the r00tz Asylum exercise was ***the first time the voting public was made aware of how fragile our election night reporting systems are to the ultimate fake news: hacked election results***. No organization can protect a website from a determined nation-state, as was evidenced by the Iranian attacks on nearly dozens of financial institution websites from 2011 to 2013. The financial industry spends billions on cybersecurity and hires some of the best cyber defenders on the planet to protect their systems. Yet even with all their resources, they could not stop a determined nation state from hacking their websites despite two years of trying. Even more disconcerting, Russia has already executed an attack on election reporting websites in Ukraine, changing results and announcing the prefered Russian candidate won when in fact he had not. Thus democracies around the world need to prepare for this threat. DEF CON is stepping up as the first organization to publicly release Election Day crisis communication protocols (below) for election jurisdictions across the globe to train in advance of Election Day.

Over 100 election officials passed through the Voting Village over the course of three days, with many training on the KIG CyberRange generously donated to the Voting Village by Cyberbit. The CyberRange is a virtualized environment allowing election officials to be trained in defending a voter registration database and simulated state-of-the-art attacks. This year the defenses of the virtual election office were beefed up by an order of magnitude from the last year's exercise. Further, to our knowledge, this is the only capture-the-flag style training available for election officials to learn how they can protect a voter registration database from attackers already in their network.

High-profile experts lined the speaking track at the Voting Village. Speakers included leaders from the Department of Homeland Security; state and local election officials, including Alex Padilla, Secretary of State of California; Noah Praetz, Director of Elections for Cook County, Illinois; Neal Kelley, Chief of Elections and Registrar of Voters for Orange County, California; Amber McReynolds, former Director of Elections for City and County of Denver, Colorado; and the senior *New York Times* correspondent and best-selling author, David Sanger. Biographical information can be found more in detail in Appendix #2.

The unprecedented attendance of election officials at DEF CON did not happen by accident. The Voting Village sent thousands of invitations via mail and email, and even made 2,500 live phone calls to election officials across the country.

---

[2] US Senate Intelligence Committee, "Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations," May 8, 2018, https://www.burr.senate.gov/imo/media/doc/RussRptInst lmt1-%20ElecSec%20Findings,Recs2.pdf.

[3] "OWASP Top 10 Application Security Risks - 2017, " *Open Web Application Security Project,* Accessed September 21, 2018, https://www.owasp.org/index.php/Top_10-2017_Top_10.

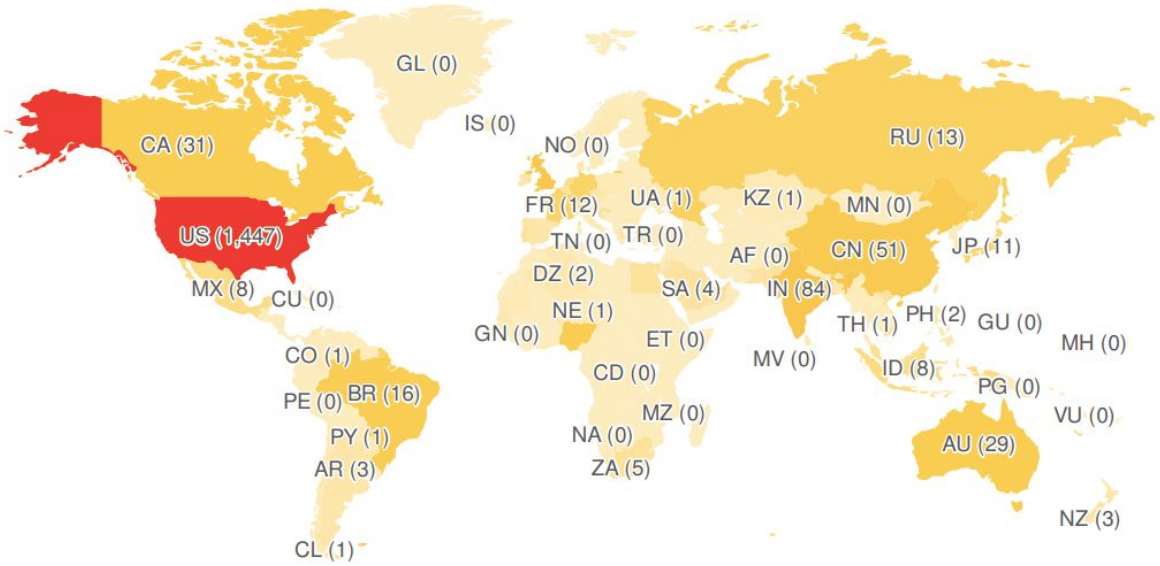
Matt Blaze, co-founder of the Voting Village, said, “It’s been incredible, the response we’ve received. We’ve had over 100 election officials come through here and they expressed over and over again how much they have appreciated learning from this opportunity.”

He went on, “Before the first DEF CON Voting Village in 2017, there were only a handful of experts on voting infrastructure cybersecurity in the United States, as well as an unknown number in Russia. Now, thanks to the efforts of the Voting Village, there are thousands of experts. Now is the time to leverage that expertise to improve election security across the United States.”

Harri Hursti, another co-founder of the Voting Village, added: “It would be extremely expensive for professionals and trained experts to match the diversity of ideas, approaches, speed, and overall creativity generated by this unorganized, large group of highly skilled people working on a common objective. The reason why many industries and government agencies have implemented bug bounty programs and other ways of crowdsourcing security work is because they are incredibly effective tools to capture this energy and innovation to help to improve their own security. For the U.S. election system, the challenges at hand are much larger than just software bugs: there are fundamental design issues to sort out and fix. The innovation inherent in this kind of exercise can be of immeasurable impact.”

Media Overview

The public and media response to the second year of the DEF CON Voting Village has been truly staggering, both in terms of its reach and in terms of the conversations it has sparked about election security. In total, the media coverage following the annual DEF CON Voting Village reached more than 2.8 BILLION people. As reflected in the Heat Map below, almost 2,000 media stories were published world wide, covering every major continent except Antarctica.



Not only did prominent publications such as *The Washington Post,* CNN, *The Wall Street Journal*, *The New Yorker*, and BBC cover the event, the Voting Village also engaged with an active audience via social media, which touched more than 146 million people. Twitter alone garnered 33,400 engagements from just one tweet on the opening day of the DEF CON Voting Village. Since July 24, 2018 and covering the dates of DEF CON, Voting Village tweets earned 1.4 million impressions, with high activity during the event itself. With a successful and active media outreach, social media accounts continued to generate interest throughout the event. With thousands of followers, the Twitter handle for the Voting Village (@VotingVillageDC) provided continual updates on what was occurring at DEF CON, engaging followers and interested parties inside and outside the event.

Other top publications that covered the event included *TIME*, *USA Today*, CNBC, *Reuters*, NBC News, *The Los Angeles Times*, ABC News, and *Politico*. Articles covered the vulnerabilities of election infrastructure and the variety of machines investigated at the event. Some news sources developed the conversation further, covering not only the threats posed to traditional election infrastructure but the rising threat of disinformation. CNN, for example, after highlighting the importance of the work being done at DEF CON, used the hacker conference as a discussion platform to voice its fear of a future influence by coordinated information warfare campaigns. Additionally, top officials from DOD, NSA, DHS and the U.S. Congress attended the Voting Village.

Equipment

The Voting Village organizers procured a variety of voting equipment for examination. The 2015 Digital Millennium Copyright Act exemption issued by the Library of Congress for good faith security research allowed Voting Village participants to find vulnerabilities without worrying about anti-circumvention liability. Prior to 2015, hackers might have faced significant liability for some of the research described in this report. Most of the equipment in the Village was purchased by DEF CON on secondary markets, such as eBay and government surplus auctions. The machines and equipment featured in the Village included:

- Dominion: Premier/Diebold AccuVote TSx
- Dominion: Diebold AccuVote OS
  This machine was lent to the Voting Village by an election official for display purposes only. Because it was needed for use in the midterm elections in November 2018, it was not used for any research or analysis by Voting Village participants.
- Dominion: AVC Edge
- ES&S: ExpressPoll Tablet Electronic Pollbook
- ES&S: M650
- AVS: WINVote
- AVC Edge activation device
- ACOSJ dual interface Java card

In addition, the Voting Village also featured the KIG CyberRange powered by Cyberbit, which provided a virtual exercise that was designed to mirror an Elections Voting Office. In a safe, virtual, and isolated network, hackers were asked to use common tools to penetrate a web application behind firewalls and manipulate records. The CyberRange exercise leveraged Kali Linux, which is a common Linux distribution including a wide range of free hacking tools and used by hackers, security professionals, and researchers today. Using the Kali Linux toolset, the hackers attempted to perform attacks like SQL Injections as a means to compromise the simulated elections office and exfiltrate the data designated as the target. However, it is noteworthy that Kali Linux offers only a small subset of the tools real cyber criminals have at their disposal. Offering Kali Linux was to facilitate participation without requiring hackers to bring their own computers and tools. However, it was also a disadvantage for the attackers as they were limited to certain tools and an environment which they may not have used otherwise.

The KIG CyberRange depends upon Cyberbit simulation technology. The Range is deployed as an isolated virtual environment, giving KIG the ability to customize network configurations to mirror real-world environments and develop unique attack scenarios.

As in the real world, the virtual exercise was not timed, and hackers were encouraged to continue trying to hack the system as long as they desired. Several made it past the web application, but none were able to penetrate the last firewall to retrieve voter records. Had hackers been successful, it is possible they could have potentially altered voter polling data – changing polling data or adding/deleting records. However, no hackers were successful in getting to the data in the simulated virtual attack exercise. It is noteworthy that this year the defenses of the virtual election office were fortified using Israeli military defense software, while attack tools were limited to what is available with Kali Linux.

The Voting Village does not manufacture opportunities for hackers to easily exploit the elections system. It is a forum for experimentation to improve the security of the U.S. elections infrastructure. The fact that no

one was able to fully penetrate the last firewall in the exercise provides useful information on a way to better protect voter data. If any state or local election official would like to better understand how the CyberRange works, please reach out to votingmachinevillage@gmail.com for more information.

Limitations

There were significant limitations of the work at the Voting Village, including:

- Participants only had access to publicly available information and the contents of the machines. In contrast, nefarious actors would not be so constrained, and could attempt to gain access to proprietary information.

- The Voting Village provided a sample of voting technologies. Organizers obtained what they could get their hands on quickly, legally, and affordably.

- The Voting Village did not provide any Election Management Systems to attendees. In a real election environment, this system is a key element as originator and aggregator of election data, and in formal studies it has been found to be the most vulnerable element, particularly in its capacity to radiate additional attack surfaces and vectors across the elections system as a whole.

- Finally, there was no access to any backend provisioning or voter registration systems. These kinds of systems are not generally available on the open market.

"Election Security is National Security"

By: Rob Joyce, Senior Advisor for Cybersecurity Strategy, National Security Agency
Originally published: *The Cipher Brief*, September 27, 2018[4]

Opinion - Many different organizations and individuals need to pull together to ensure we have secure and trustworthy elections. The distributed nature of our elections throughout the state and local governments means there are widely varying levels of expertise and resources available, even when state and local officials leverage the federal government for support. This election infrastructure can be expansive, and includes the voting machines themselves, the tabulation processes, the voter registration databases and the associated networks. Each of these requires a detailed focus from many entities to protect against adversaries seeking access to data for influence operations, threatening the availability of the services, or posing threats to the integrity of the information.

I recently caught a glimpse of the kind of offensive focus I'm talking about at the Voting Village at DEF CON 26. I witnessed private individuals donating their time to improve the security of our election processes. They've made incredible contributions, and are offering advancements for federal, state, and local election programs, as well as insights for the manufacturers of voting technology. Strongly connecting all the contributors to our election process needs to be a goal for improving election security. These connections are vitally important to ensure everyone is aware of the threats, best practices and needed improvements.

Amazing talent and expertise gathers at DEF CON with an enthusiasm to make things better. The combination of skilled cybersecurity experts in partnership with industry and the ultimate end users of the technology – state and local election officials – is a powerful alliance. . . . Steering the voting village to similar collaborative relationships will take us to the next level and address the constant erosion of trust, which only helps further the objectives of our adversaries.

Ignorance of insecurity does not bring you security. As time passes, the security of any device begins to erode. New exploitation techniques are developed. New investigative tools are created. Zero days are discovered in operating systems. The capabilities and repertoire of the exploiters grows. Developers of the security models for a device can never predict every creative idea that will be tried during exploitation. For these reasons, we need to continuously red team our devices and processes. This independent testing provides great benefit by straining assumptions and uncovering hidden flaws.

Another key aspect of securing our election processes is simply focusing on the fundamentals. As we embrace electronic technology, the basic security practices of updating and patching are critical. Having strong adherence to recommended security design practices is vital. Often, paying attention to detail in the things that we already know how to do, removes significant risk.

While DEF CON continues to foster a venue to investigate election infrastructure in the Voting Village, the focus cannot simply be about calling out the state of security in our current technology. Rather the result needs to be developing tangible actions that lead to collaborations that will make us more secure.

[4] Joyce, Rob. "Election Security is National Security." The Cipher Brief. September 27, 2018. Accessed September 27, 2018. https://www.thecipherbrief.com/column_article/election-security-is-national-security.

Election security is a matter of national security, and there's no question that progress has been made since 2016 – government-industry partnerships exist today that simply did not exist even a year ago. These security-focused engagements between election officials, the federal government, and vendors will undoubtedly contribute to making the 2018 mid-terms the most secure elections in recent memory. But there's more to be done, and securing our elections is like a race without a finish line. Together as a community – hackers, government and industry – can bring powerful assurances to a foundational component of our freedom: fair and trustworthy elections.

Technical Findings

Diebold ExpressPoll-5000
The Diebold ExpressPoll-5000 is an electronic pollbook, designed for use by individual pollworkers. It is used in precincts to check voters in before they are permitted to vote. The product line currently belongs to ES&S, but the ones used at DEF CON were models running Diebold-branded software, which is also still in use in several places in the U.S. Its operating system is a version of Windows CE, a system built by Microsoft for embedded applications. The pollbook application software was version 2.0.27. The data in an ExpressPoll-5000 is stored on a removable Compact Flash card with additional ability to utilize PCIMCI cards.

The principal investigators of the ExpressPoll-5000 machines at DEF CON were Miguel S., a software engineer, and Akin O, a Nigerian application software security engineer. These investigators were able to access the file system and read and write the voter databases using SQL Lite, a free database program widely available. The investigators found entries in the database where the passwords to the ExpressPoll-5000 were stored in cleartext.

The root password for the machine was “password”.

The admin password was “pasta”.

There are several security mistakes here if a jurisdiction is serious about security. First, the root password is apparently unchanged from the operating system default. When setting up a new machine the first thing one should always do is assign a new root password. It also is extremely bad practice to store passwords *in the clear* (i.e. unencrypted) and in a place that will ever fall into someone else’s hands (as this ExpressPoll-5000 did). Presumably any poll worker in the jurisdiction from which this machine came can use the passwords to gain control of the machine and make arbitrary changes to it.

The admin password, “pasta”, is probably not the default password, i.e. it probably was changed to that when the machine was configured. But it is a poor choice because it is short, all lower-case, and contains no digits or special characters. More significantly, it does not matter what the admin password is if the root password is the default value, since the root user has more privileges than the admin user. Additionally, it demonstrates that Federal Information Processing Standard rules, as defined by the National Institute of Standards and Technology (NIST), are not enforced by the software.

Dominion AVC Edge
The AVC Edge is an electronic voting machine manufactured by Sequoia Voting Systems, later acquired by Dominion Voting Systems. It is a touch-screen machine with direct-recording electronic capabilities. It is activated by a smart card, and records votes on internal flash memory. Each unit contains a slot for a vote activation card. After the voter’s ballot is cast, the smart card is deactivated to prevent multiple votes from being cast. Votes are subsequently documented. When polls close, the votes recorded in each machine are either physically or electronically relayed to election headquarters. It is currently in use in Arizona, California, Florida, Illinois, Louisiana, Missouri, New Jersey, Pennsylvania, Washington, and Wisconsin.

As the whole execution environment is stored on the removable storage device with no permanent physical security protections in the form of locks or even tamper-evident seals, researchers were able to simply open the machine’s outer casing with common screwdrivers, gain access to the storage device slot, and

swap the device with a new device with a different operating system installation and application. Tamper-proof seals specific to a particular election would not protect against this, as an attacker would only need to swap out the removable media once during the lifetime of the device.

In the Voting Village the removable media were replaced with new media with completely different programming to verify that there were no security measures, such as secure boot or cryptographic signatures, preventing the device from accepting arbitrary new programming. Though old, the AVC Edge hardware is common; therefore there are no obstacles to creating rogue software deployments for the device.

Dominion Premier/Diebold AccuVote TSx

The AccuVote TSx is an electronic voting machine manufactured by Premier Voting Solutions, later acquired by Dominion Voting Systems. The product line currently belongs to ES&S, but it is unclear if the machines used at DEF CON are Dominion or ES&S products. The AccuVote TSx is currently in Alaska, Arizona, California, Colorado, Florida, Georgia, Illinois, Indiana, Kansas, Missouri, Mississippi, Ohio, Pennsylvania, Tennessee, Texas, Utah, Wisconsin, and Wyoming.

During DEF CON, the Voting Village organized a mock election to demonstrate vulnerabilities in the AccuVote TSx. The software used in the demonstration was unmodified from the software that is still used widely. Additionally, there are older, potentially more vulnerable versions of the software still in use.

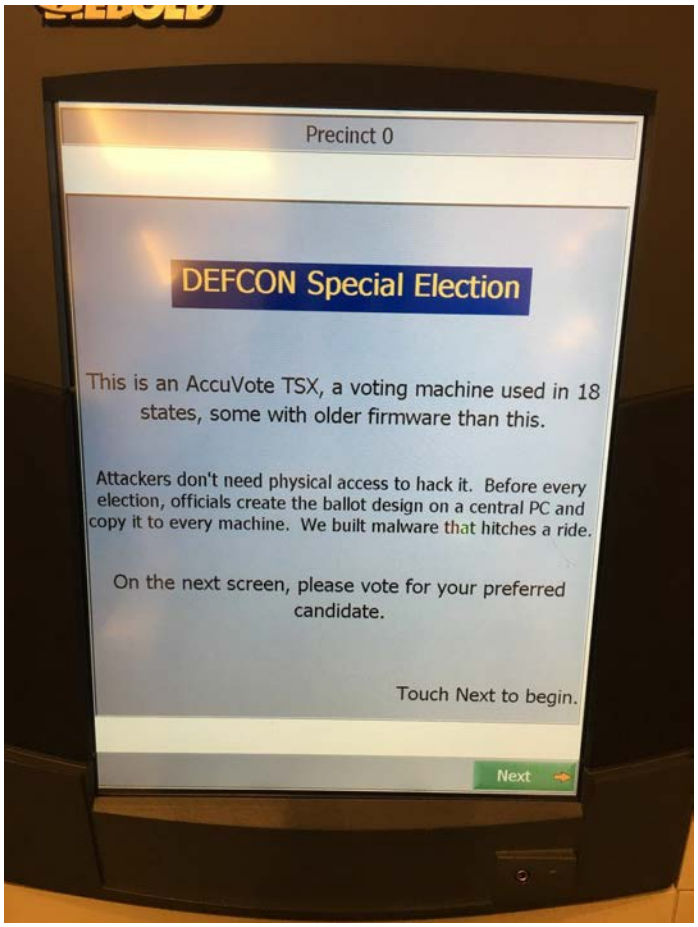
The mock election demonstration consisted of multiple elements:

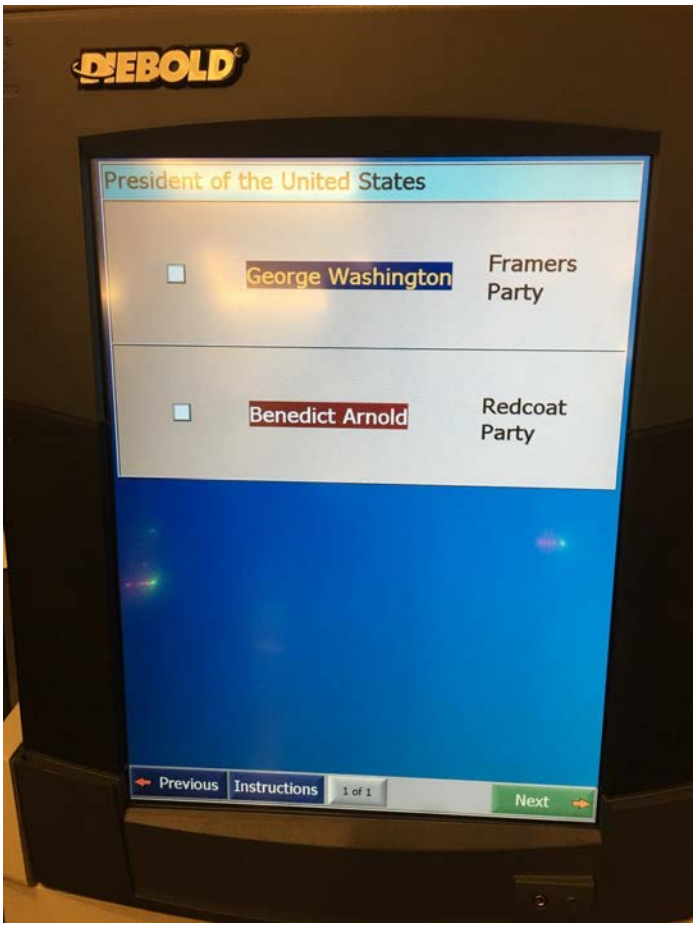
- All voters used the same voter activation smart card without the card being reactivated with a device of any kind to allow the next voter to cast their ballot. This is because the voter activation card was programmed to automatically reset itself after activating the device, therefore allowing it to be used to cast unlimited number of ballots.

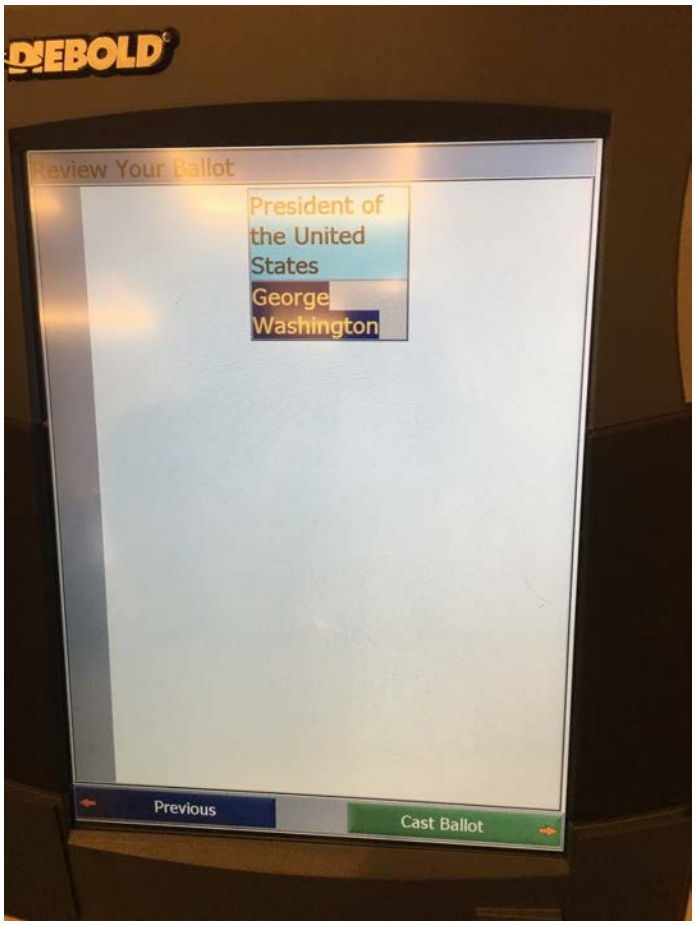
- The election was programmed without using software provided by the vendor, therefore proving that a chain of custody of the election management software does not prevent new elections from being programmed. This also indicates that third parties with no access to the election management system can create rogue election definitions which are indistinguishable from real elections.

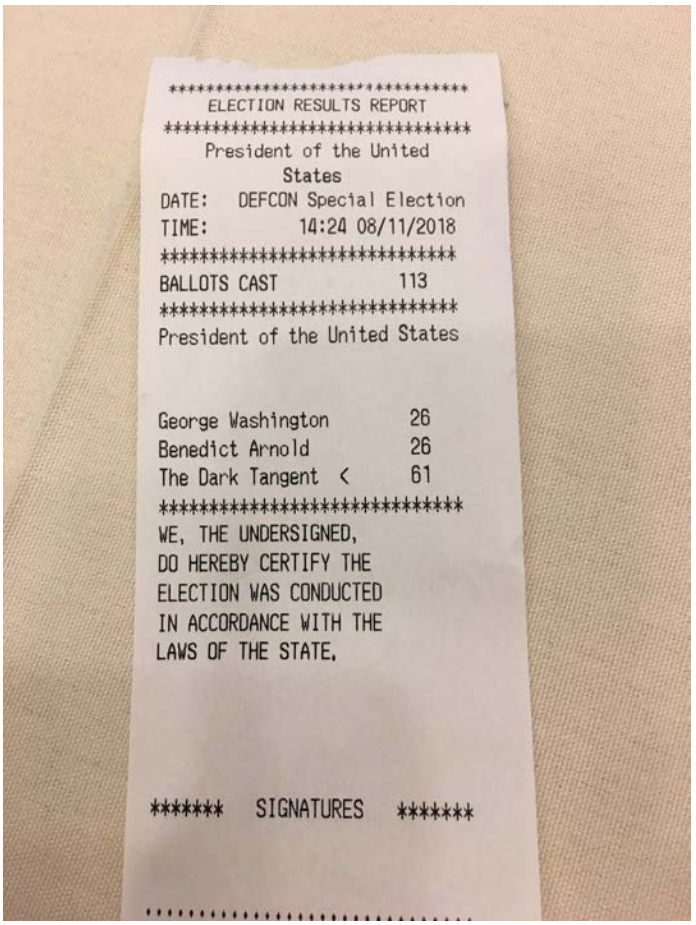
- An attack can be distributed remotely with no physical access to the voting machine. Malware needed in this demonstration can be distributed with the ballot/election definition. This also demonstrates the mechanism enabling a wholesale attack. Depending on how a particular county's system is set up, there may be multiple centralized systems in the chain of the information flow to the voting machines, and compromising any of the links in the chain enables a wholesale attack.

- Paperless, unauditable systems are extremely vulnerable to this kind of attack, as the only record of a voter's intent is in digital form.


Precinct 0
DEFCON Special Election
This is an AccuVote TSX, a voting machine used in 18 states, some with older firmware than this.
Attackers don't need physical access to hack it. Before every election, officials create the ballot design on a central PC and copy it to every machine. We built malware that hitches a ride.
On the next screen, please vote for your preferred candidate.
Touch Next to begin.
Next


DIEBOLD
President of the United States
George Washington
Framers Party
Benedict Arnold
Redcoat Party
Previous
Instructions
1 of 1
Next


DIEBOLD
Review Your Ballot
President of the United States
George Washington
Previous
Cast Ballot


ELECTION RESULTS REPORT
President of the United States
DATE: DEFCON Special Election
TIME: 14:24 08/11/2018
BALLOTS CAST 113
President of the United States
George Washington 26
Benedict Arnold 26
The Dark Tangent < 61
WE, THE UNDERSIGNED,
DO HEREBY CERTIFY THE
ELECTION WAS CONDUCTED
IN ACCORDANCE WITH THE
LAWS OF THE STATE,
******* SIGNATURES *******

As a surprise, the largest social media visibility from the village was for viral video posted by social engineer Rachel Tobac. At the time of writing, the video (https://twitter.com/racheltobac/status/1028437783050776576?lang=en) has been viewed over 2 million times. While this hack that Tobac demonstrated was known before DEF CON, we revisit it here in light of the renewed public attention. The AccuVote TSx voter activation smart card reader unit is held in the place by a flimsy piece of plastic which can be easily pulled from the main casing and re-installed. The process requires no tools, very little physical force, and can be done in a matter of seconds within the privacy shield of the voting machine. By separating the piece, an attacker gets access to the connector cable of the reader unit. If an attacker disconnects the cable, during the next start-up the voting terminal will allow the attacker to enter the system settings dialog without any authorization checks. This vulnerability allows an attacker to potentially disrupt the election process, but based on the current understanding will not affect the integrity of the votes.

ES&S M650

The M650 is an electronic ballot scanner and tabulator manufactured by ES&S. The ES&S M650 is used for counting both regular and absentee ballots. It launches ballots through an optical scanner to tally them, and keeps count on an internal 128 MB SanDisk Flash Storage card (pictured below). Election staff are responsible for configuring the M650 for each election. It is currently in use in Arkansas, California, Florida, Idaho, Illinois, Indiana, Kansas, Minnesota, Missouri, Montana, North Carolina, Nebraska, New Jersey, Ohio, Oregon, Pennsylvania, South Carolina, South Dakota, Tennessee, Texas, Washington, West Virginia, and Wyoming.

The M650 runs QNX 4.2* on an Octagon 5066 Board with an AMD Am5x86 processor at 133MHz. QNX is a Real Time Operating System (RTOS) that has some loose parallels to modern-day Linux and Unix operating Systems. The version of QNX running on the M650's at DEFCON was last updated in 2008, and QNX 4.2 was released in 1996.

Physical Security

There is a common misconception that physical security precautions (tamper-evident seals, locks, etc.) keep voting machines safe from malicious attacks. While all equipment was shipped to us with keys, the researchers wanted proof that the locks in the machine did not inhibit access. In under a minute, a Voting Village researcher picked the lock on the back of the M650 (pictured at left) and unlocked its case, gaining full access to the computer systems and electronics via a serial connection to the main board. Features of note include two OKI Microline 9-pin dot matrix printers connected to two exposed parallel ports, an exposed ethernet jack, and a ZIP disk reader/writer. There was no other type of tamper-evident security on the machine. Physical security such as this lock, even in a small county office, is not sufficient to protect voting systems.

Serial Terminal

With a $10 adapter (VTC-9F to DB-9 adapter cable, item 1041), a serial connection can be established to the M650 by connecting to the main 5066 CPU board. The connection is extremely simple to establish, as it uses the default serial parameters for popular, free programs like Putty and TeraTerm (Windows), as well

as Linux commands like `screen` (where the only requirement to successfully opening a serial console is specifying a baud rate of 9600). Connecting a laptop allows root access to a serial terminal session with username 'root' and no password. There is not even minimal account security.

From this connection, an attacker can tamper with election data. All these data are stored in `/flshdr/elecdata`, the mount point for the 128MB SanDisk Flash Storage device that is on a standalone board inside the M650 computer board cage. An attacker could also conduct a denial of service (DoS) attack against the system, or display any message to the screen or printers connected to the computer.

Furthermore, there exist commercially available tools which can be used to automate an attack of this nature, as well as small, commercially available devices which can be installed into this interface to enable remote and wireless access to this port. Because the serial is not used during normal operations, adding such a device without detection is possible. Researchers estimated that it would take one to two minutes to pick the lock, carry out the installation of the attack and relock the device.

Ethernet Port Vulnerability

The ES&S M650 voting machine has two communication media options - Ethernet connection or Zip drive. On the side of the M650 is an RJ45 jack. This connection allows the M650 to send data over a network to a system running ES&S Unity, the election management system software.

During bootup the M650 makes a DHCP request to obtain an IP address using the DHCP client provided in the QNX TCP/IP module, dhcp.client. This DHCP client shares a substantial amount of DHCP protocol handling code with the ISC DHCP server version 1.0.0, although the client-specific portions seem to be closed source. Version 1.0.0 of the ISC DHCP server has several known buffer overflows. However, we were not able to trigger these overflows with server-provided data in this client implementation.

After obtaining an IP, the M650 sends a packet on port 6500 to the Unity server expected at a fixed IP address. This initial packet carries the following hexadecimal payload: `01 00 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00`. The significance of this message (which is part of one of the TCP packets) is currently unknown.

Zip Disk Vulnerabilities

A second investigation of the M650's vulnerabilities revolved around the Zip drives and Zip disks used on the machine. The Iomega products that are used by the M650 are an old and obsolete removable disk technology. Zip disks were intended to be treated as if they were a "fat" floppy disks, but with a much larger capacity (100 MB or 250 MB compared to the 1.44 MB capacity of a common 3.5 inch "high-density" floppy).

There are eight different types of Zip drive devices, and each is different in terms of electronics, storage capacity and other aspects. As an added layer of complexity, the description of a 'super floppy' is an operating system-specific description, referring to Windows. Other operating systems commonly see the drive as more like a removable hard drive. In the M650 operating environment "Unity," the election management system uses a Windows Operating System while M650 itself uses QNX as its operating system. (Voting Village participants did not have access to Unity software.) Therefore they see and operate with the

drive and the file system(s) on it in an inconsistent way. The main difference is that a super floppy is a single file system, while the disk is not subdivided into separate sections, called partitions, which can not see each other - the hard drive type of media includes a partition table, which means that the disk can have multiple separate file systems. If the machine mounts one of the partitions assuming it is the whole disk, the computer will not be aware of the other file systems or the files stored on them.

As stated previously, the Zip drive's primary purpose is to store and transfer the election specific definitions and, ultimately, the results. However, the Zip drive also has the ability to alter or replace any and all of the programming stored on the internal storage devices. This kind of attack is called an advanced persistent threat (APT). APTs are a family of stealthy and continuous computer hack processes designed to be hard to detect, hard to clean, and potentially virally propagating.

On bootup, the M650 executes a startup script called "`sysinit`" (stored on the flash storage device, under `/flshdr/sysinit`). The `sysinit` script is run on every boot-up of the M650. It is responsible for starting drivers, mounting storage locations, and initiating an update. To decide if an update will be run, the machine runs this line:

```
if [ -f /dos/a/<redacted_1> -a -f /dos/a/<redacted_2>.etp -a -f
/dos/a/<redacted_3> ] ;
```

Although we have redacted the file names, they are all single, commonly used English words that can be easily guessed from the context.

In this line—one of the two checks required to perform an update—the machine runs a file presence check (`-f <file>`) on three files (`<redacted_1>`,`<redacted_2>.etp`, `<redacted_3>`) that should be on the zip disk (mounted as `/dos/a/`) to move on to the next step of running an update. This next step is even more trivial: a version check. The `sysinit` script, provided that it finds the three files listed above, runs this line to "check" version numbers:

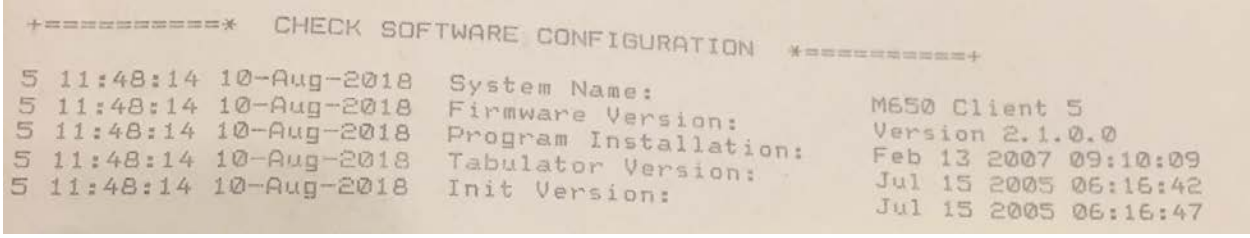
```
if [ "$new_vers" != "$curr_vers" ] ; then
```

This line simply ensures that the new version of software (read from `/dos/a/<redacted_2>.etp` on the zip disk) is *not the same as the existing version* (thus the use of the `!=` operator). The existing version is stored in (`/flshdr/<redacted_2>.etp`). By using the "`!=`" operator, the software could theoretically be downgraded as well as upgraded: a lower software version on the Zip disk would still make that "`if`" statement true. Following these two trivial and insecure checks, the machine continues to copy the update script to the root directory (`/`) and then runs:

```
display "Updating firmware to $new_vers."
/<redacted_1> &
```

Through this function, the machine checks for the presence of "`<redacted_1>`" (any script), "`<redacted_2>.etp`" and "`<redacted_3>`" on the Zip disk (mounted as `/dos/a/`) and, provided that the versions are dissimilar, runs the update script without checking any further. The lack of checks here would allow a knowledgeable attacker to run an arbitrary script on the machine - no integrity checks, passwords, or signatures are performed on any file from the Zip Disk (including the `<redacted_2>` script itself). The system also lacks any kind of potentially security-enhancing subsystems like sandboxing. If the

M650s are networked at the clerk's office, this vulnerability would allow a malicious actor to spread malware across the network, possibly infecting other machines.



Zip drives and Zip disks are discontinued end-of-life products, but the M650 depends upon this technology for loading and updating its software and firmware. This causes a number of serious security vulnerabilities. If a Zip drive in an M650 fails, it is difficult to replace. However, the Zip disks are even more problematic. Often jurisdictions have to buy them used, which means that they have already been formatted, probably on a Windows machine, and they may have files already recorded on them. Even if bought from Amazon, they in turn may have been purchased from random eBay sellers.

A Windows-formatted disk can be read by a machine running QNX. Thus, a used Windows-formatted Zip disk with files recorded on it will appear to work normally when inserted into an M650. But this necessary and useful capability opens the door to a serious security vulnerability.

The two operating systems, Windows and QNX, use different device drivers, volume drivers, and file system implementations. In fact, the QNX operating system is not on the list of officially supported operating systems for Zip disks, so presumably someone originally ported the Zip software from yet another platform, possibly Linux, with an unknown level of testing and skill. This leads to the possibility of differences in the two operating systems' use of Zip disks, and we know such differences exist at least in their handling of partition tables on Zip disks. Generally, with independent implementations on different platforms of the "same" software one always expects different behaviors in corner cases, different bugs, and different error behavior, leading to security vulnerabilities when the implementations attempt to interoperate.

One major potential security vulnerability arises from the possibility that used disks originally written on a Windows or Mac machine might be procured and used on the M650 without being reformatted. In that case the differences in operating systems provides a potential vector for attack. As described elsewhere in this report, a Zip disk is used to update the software of the M650. If there is an executable file named "update" on the disk at the time the M650 is booted (and a couple of other simple conditions are met) then the M650 will immediately run the update program. Normally the update program would install a new version of the code running on the M650, but it could do literally anything else, including inject malware to miscount votes or inject a virus that could spread among all the M650s in a jurisdiction through the exchange of Zip disks.

A clever attack on an election would start by the attacker writing a malicious QNX executable file named "update" on a bunch of Zip disks and giving those files the Windows attributes `hidden` and `system`. Then the attacker could find a way to offer those malicious disks for sale to a jurisdiction that needs more Zip disks and is having trouble buying brand new ones.

If an IT person inserts one of the malicious disks into an M650 without reformatting it first, the update file

will immediately and silently install the malicious software into the M650, thereby undermining the integrity of the election. If the IT person took the precaution of examining the contents of the Zip disk first, he or she would see nothing because the files have the `hidden` attribute. If he took the further precaution of issuing a command to delete all files from the Zip disk, the malicious files would not in fact be deleted because they are marked with the `system` attribute. Only if the disk is reformatted on a known clean machine before being inserted for the first time into an M650 would the malicious update file be destroyed.

It is very doubtful that the operators of M650s all over the U.S. are aware of the necessity of this precaution of reformatting every Zip disk before using it in the M650. As the M650s get older and Zip disks become scarcer, this vulnerability grows in importance.

This is an example of a broad class of vulnerabilities that are well-known in the computer security world — `autoplay` or `autoexecute` features in removable storage media alongside with Master Boot Record and other types of lower level attacks. We have seen attacks like it before with the auto-update feature in Diebold voting machines through their memory cards, and similar capabilities in other vendors' voting machines. We have also seen it historically with autoexecute features in CD drivers, in email clients, and in thumb drives (the latter believed to be one of the ways Stuxnet was introduced into the Natanz uranium enrichment facility in Iran). But the new feature here is that the scarcity of obsolete Zip disks will drive M650 jurisdictions to buy them from second-hand sources. Such disks must be treated as contaminated, even if they appear clean.

In other words, the M650 is simply looking for a file with a certain file name and is trusting it and executing it with the maximum level of privileges, which has never been an acceptable practice from a security point of view. This practice is made more dangerous because the different operating systems involved in making data hygienics difficult and making it possible to hide critical files, and even complete file systems, and making those potentially able to survive many commonly utilized methods of erasing content.

If the machines are disconnected from a network the attacker could initiate the printout of a false report from the report printer or Zip disk - the means used to record the totals. Of course, the attacker can also, through this vulnerability, change election data stored on the machine and create matching false digital records to be reported to the central tabulator.

Any of these vulnerabilities seriously compromises the integrity of an election. They require no passwords and necessitate only basic knowledge to successfully complete. **The dangerous update procedure was documented but file names were redacted in the 2007 EVEREST report because of the grave security risk.**[5]

Mitigation against this combination of factors would require additional measures for the secure cleaning of all residual data from the drive on the lowest level possible - not only when the drive is put into use, but also between every instance it is used in order to prevent a viral attack to utilize the drive as a distribution media in and of itself. All storage devices or removable media should be formatted before first use in any machine that is part of, or networked with, any voting system. This has to be a routine precaution faithfully practiced. Injection of malicious software through unclean media is one of the ways that it is possible to hack voting systems that are not connected to the Internet. Isolating a voting system from the Internet is

[5] Pennsylvania State University, the University of Pennsylvania, and WebWise Security Inc, EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing. Compiled by Patrick McDaniel. By Matt Blaze and Giovanni Vigna. December 7, 2007. Accessed September 25, 2018. https://www.eac.gov/assets/1/28/EVEREST.pdf.

necessary to protect it, but it is not sufficient. Malicious logic can enter by other means, and only careful diligence (or luck) can prevent it.

Cross-Device Vulnerabilities: Smart Cards

Several types of voting machines, including the Dominion Premier/Diebold AccuVote TSx and the Dominion AVC Edge, use smart cards to enable voters to vote on Election Day. Smart cards are commonly also referred as Java-cards, as the chip on the card is a low-powered computer which runs programs written in Java, a common programming language. When the card is plugged in, it gets its power from the connection to boot up. Once up and running, the card starts to communicate with the host computer. In the election environment, the smart card is set up for the voter to cast their ballot either by an ePollbook, such as the ExpressPoll 5000 (discussed above), or by a specialized programming device called Voter Card Encoder (VCE). It can also be used to select the voter's ballot.

Researchers in the village were able to set the VCE device to a mode accepting a new program image to be flashed in, completely replacing the old programming. However, the researchers ran out of time to create malicious demonstration image for the device. Installing new software on a VCE does not require any authentication or check mechanisms. Simply by pressing the "Off" button, the device will query if the user wants to upload a new software image.

Advances in electronics have enabled the power consumption of the chip to be reduced greatly enabling the chip to be powered wirelessly over Near-field Communication (NFC) without a physical connection. These cards are called dual-interface cards and have both a physical chip interface and a wireless NFC interface. These cards are readily available for purchase and retail for about $20. Modern mobile phones have NFC capability built-in, meaning that dual-interface cards are field-programmable by simply using a mobile phone as the programming device over wireless. The same programming is also able to communicate over the physical chip connection.

Due to a lack of security mechanisms in the smart card implementation, researchers in the Voting Village demonstrated that it is possible to create a voter activation card, which after activating the election machine to cast a ballot can automatically reset itself and allow a malicious voter to cast a second (or more) unauthorized ballots. Alternatively, an attacker can use his or her mobile phone to reprogram the smart card wirelessly. All elements of the system seem to accept smart cards with the hardcoded default password (0x01,0x02,0x03,0x04,0x05,0x06,0x07,0x08). Among other factors, the obviousness of the password makes forging smart cards easy. This password has been previously published as part of the EVEREST report in December 2007.[6]

In addition to allowing a malicious actor to vote more than once in jurisdictions where the voting terminals have more than one ballot style available, the modification of the voter activation card could also enable the malicious actor to cast multiple ballots, including for races for which the attacker is not eligible to vote at all.

In-flight Email Ballot Modification

Over thirty states allow at least some voters (usually overseas and military voters) to cast ballots as

[6] Pennsylvania State University, the University of Pennsylvania, and WebWise Security Inc, EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing. Compiled by Patrick McDaniel. By Matt Blaze and Giovanni Vigna. December 7, 2007. Accessed September 25, 2018. https://www.eac.gov/assets/1/28/EVEREST.pdf. Page 145.

attachments to an email message. This is an extraordinarily dangerous practice because email is not end-to-end encrypted, not authenticated, its headers (including the "From:" and "Date:" lines) are forgeable, and offers only "best effort" delivery, i.e no strong guarantees. Email is not remotely a secure transmission medium. Anyone who controls an email forwarding agent or email server is in a position to modify, copy, re-route, or discard any ballots he does not like. And since the ballots must be accompanied by the name of the voter, the secrecy of a ballot transmitted by email is totally compromised. Two DEF CON investigators helped demonstrate one of the innumerable kinds of potential attacks on email ballots.

The two principal investigators of email ballot modification at DEF CON were both researchers at Free & Fair, a company that provides open source elections services and systems: Dan Zimmerman, Principled Computer Scientist, and Lyell Read. Their investigation was not of any particular machines, but of general vulnerabilities inherent in email voting. In the past, Dan Zimmerman has demonstrated how a home router could be hacked to intercept an emailed ballot before it even leaves the voter's home. The malicious code in the router could modify votes arbitrarily, with neither the voter nor the election official running the server having any way to detect the problem.

In this case, the investigators demonstrated a similar hack, but instead of attacking the sending side of the communication, they attacked the *receiving* side, inside the email server such as a jurisdiction's election agency might run. They assumed that an emailed ballot consisted of three JPEG images attached to an email message, presumably to contain voter ID and authentication information, a signed oath or affirmation, and the voted ballot itself.

A modern email server has hooks to allow linking with "filter modules." The purpose of filter modules is to allow preprocessing of an email before it is delivered to the final recipients. Such modules are commonly used for spam filtering and other purposes, such as disabling URLs embedded in the email, stripping executable attachments, auto replying with a vacation message, blocking certain senders, apply classification rules, etc. An email filter can be written to do literally anything with an incoming message before it is delivered to the addressee.

The investigators wrote an email filter that modified the JPEG attachment that contained the incoming ballot. Technically the filter was a BASH script that ran the ballot through ImageMagick (an open source Linux utility for editing images) and used its `Convert` command to swap two known ovals on the ballot, before replacing it as a message attachment and delivering the email to the recipient's Inbox. The swapping of the two ovals, which represents moving a vote from one candidate to another, is just an example of the kind of arbitrary vote manipulation that could be done in an email filter. The malicious processing of the ballot would probably delay its delivery by a few milliseconds — essentially unnoticeable.

The programming of the demonstration was completed in approximately two hours, start to finish.

This hack illustrates how vulnerable email voting is to undetectable manipulation while in transit. A rogue individual (and it can easily be a single person) who maintains the email server can write and install such a filter module and later remove it after the election. It would be difficult to detect that the email ballots were manipulated to reflect the programmer's vote choices because neither voters nor election officials will see anything suspicious.

Alternatively, the email server might be remotely hacked by anyone on the Internet — criminals, domestic partisans, or foreign intelligence agencies. The hackers might install such a filter (and later remove it) and thus control the outcome of the election.

Forensic Studies - AVS WINVote

The AVS WINVote machine is an electronic voting machine manufactured by Advanced Voting Solutions (AVS). It possesses a touch-screen voting terminal, a full color screen, as well as zoom capabilities. It is equipped with a wireless local area network and battery backup power, a printer, and modem. The AVS WINVote stands supported in a voting booth and was designed to function as a stand-alone system and it can be used as both a precinct voting device and as a non-geographic station. WINWare is the software used for election management in the WINVote system. As of the 2016 elections, the AVS WINVote is no longer in use.[7] Its reputation as "America's worst voting machine" is well-documented[8] and well-deserved.[9] Given the surfeit of information available about the WINVote's many vulnerabilities, this report will focus on new discoveries as reported at BlackHat 2018 by Carsten Schurmann, Associate Professor at the IT University of Copenhagen, and as uncovered at the DEF CON Voting Village.

The AVS WINVote machines used at the DEF CON Voting Village originally came from Virginia. The principal investigators at the Voting Village were Carsten Schurmann and Will Baggett, a computer forensic examiner. They were assisted by Minoo Hamilton, a security engineer.

The WINVote machine runs an early version of Windows XP from 2002. It thus has none of the updates (Service Packs 1, 2, and 3), bug fixes, or security patches that were offered by Microsoft in the seven subsequent years that the operating system was supported. Application of updates would require recertification of the whole system (according to Virginia law and practice).

In addition to one physical machine, the investigators had access to a total of 16 NTFS file system images from a total of eight WINVote machines, all from machines that had been used in Virginia for years, so they were able to do some comparative studies. At the end of DEF CON the investigators were still studying the WINVote system and the file system images, so this report is only inclusive of what they had discovered as of the end of the conference.

The investigators used the free forensics tool Autopsy to examine the file system images to look for anomalies. They also used various Windows utilities and a forensic undelete utility that could recover files that had been deleted but not overwritten.

Music software and music file

The first discovery that Schurmann made was that four of the eight machines investigated showed evidence of being used for ripping and playing music. The machines contained a copy of coolplayer.exe, an MP3 player program. One possible legitimate use of this program would be to play audio for blind voters, though there is no indication that this is the reason the program was added. However, the machines also had a copy of the "No1" CD-ripping program, a program used to copy music from an audio CD and store it as MP3 files. The WINVote does not have a CD drive, so one would have to plug a CD drive into the USB port on the

[7] Jeremy Epstein, "Decertifying the worst voting machine in the US," *Freedom to Tinker*, April 15, 2015, https://freedom-to-tinker.com/2015/04/15/decertifying-the-worst-voting-machine-in-the-us/.

[8] Virginia Information Technologies Agency, "Security Assessment of Winvote Voting Equipment for Department of Elections," *Wired*, April 14, 2015, https://www.wired.com/wp-content/uploads/2015/08/WINVote-final.pdf.

[9] Shaun Nichols, "Default Admin Password, Weak Wi-Fi, Open USB ports ... No Wonder These Electronic Voting Boxes are Now BANNED," *The Register,* April 17, 2015, https://www.theregister.co.uk/2015/04/17/virginia_nixes_highly_pwnable_voting_boxes/.

machine to use this program. There is evidence that this is exactly what happened at some point, because on the same four machines the investigators found copies of a Chinese-language pop song, the same one on each machine.

Since the same Chinese-language song was found on four different machines, this indicates that the song was copied onto the machines at the time the master software distribution for the WINVote was being built, i.e. from before the machines were delivered to Virginia. Most likely an engineer (presumably someone from China, or at least someone interested in Chinese music) was configuring the master software for the WINVote and also ripping CDs and listening to music while doing so. When the engineer committed the final software configuration he failed to erase the music, the MP3-player, and the CD ripper, and they were distributed along with the rest of the voting machine software to at least one jurisdiction in Virginia.

The Virginia jurisdictions that received the machines with the music and CD ripper probably never examined the application software that was installed on the machine. They apparently just accepted the system as delivered and used it for several years. There is no telling what other software, possibly malicious software, may have been installed on the WINVote machines that Virginia officials never noticed in the approximately ten years they were in use. Needless to say, the presence of such rogue files within the software image can only happen with extremely careless and unprofessional development practices and with complete negligence or disregard of any known best practices and quality controls.

Records of past elections
Aside from the musical discovery, the investigators found records from numerous past elections stored in a Microsoft Access Database (.mdb) file in the file system images. There were lists of candidates, voted ballot images, and vote totals. There is nothing inherently wrong with retaining data from past elections in a voting machine, since the data is not confidential, but it is a very poor management practice. First, Microsoft Access has notoriously weak security, which would not be an important point if the machines were forever isolated. However, these machines have WiFi connectivity, and as we describe below, there was clearly no prohibition on connecting the machines to the Internet.

Second, it shows that for many years the file systems of the machines were not re-initialized. The best practice would be to reinitialize the software at least once for each general election, if not for every election. That way errors in the file system do not accumulate, and any bad registry entries, bad data files (caused by I/O errors or power outages), or any software, especially any malicious software, that may have been installed since the last use would be wiped clean for the next election.

Finally, the fact that this data from past elections was still present on the voting machines as acquired by the investigators indicates that the machines were not wiped before they were disposed of by the Virginia jurisdictions that used them. It is always good practice to wipe a file system before disposing of a machine.

Log files show election data had been transmitted over the Internet to a third party
On at least one of the machines there are log files showing that the entire database of an election was transmitted to a third party company. It was transmitted via FTP, unencrypted and unauthenticated, to the IP address 184.69.193.146 which belonged to a server named ftp.enfocom.com. That server is still online. Today the Enfocom International Corporation is a technology company located in Calgary, Alberta, Canada, and its mission is “To be the leader in providing technology solutions in secure network services and secure software products.”

Since the data in the WINVote database is not confidential, the transmission to Enfocom does not

necessarily represent any kind of privacy breach regarding the data itself. The investigators just do not know why voting data would ever be transmitted to any third party, or why they were transmitted to Enfocom in particular. The investigators also do not know whether the IP address they used was located outside the U.S. at the time of the transmission. They did determine that apparently that particular IP address is no longer associated with Enfocom, though that is not necessarily significant.

However, the log clearly shows that there was a direct FTP connection from a voting machine to a distant server over the Internet. This is a potentially disastrous security blunder because it could enable external attackers to penetrate and control the voting machines. Established best practices are that voting machines should *never* be connected to the Internet, even briefly. This is especially true of systems running old, unpatched Windows XP, which are often penetrated and infected with malware within a few minutes of their first connection to the Internet. Furthermore, from a basic operational security point of view, discontinuing the use and blocking of unsafe protocols like FTP has been recommended for years prior to the log entries found, further demonstrating that the baseline external security measures have not been in place at all, or were deeply flawed. These log entries cast doubt upon the claim that election environments are shielded from hostile environments with external security mechanisms.

Deleted files
The investigators ran a forensic "undelete" utility on one of the WINVote images and were able to recover 1764 deleted files, i.e. files which were put in the Windows Recycle Bin, and the Recycle Bin emptied, but the files were never overwritten. When examined, the files appeared to be routine information, including:

- change logs for years of changes
- photos of components
- a ringtone (modem noises)
- a deleted copy of the Windows registry
- .zip file of cast vote records
- an external drive insertion log
- a directory named "crypto"

The investigators did not have time to examine these files any further, but nothing appeared suspicious. The existence of these deleted files is, however, further evidence that the file system had never been re-initialized in the many years the WINVote machine was in use.

Physical vulnerabilities
A fourth major vulnerability was discovered by Mixael (pseudonym), a mathematician who was also working on the WINVote machines. In this case, the investigator noticed a simple keylock on the front panel (faceplate) of the WINVote. He applied the simplest lock picking tool there is, a "jiggler key." A jiggler key is a simple metal key cut from a totally flat blank with one or more generic bumps along one or both edges. It is not specific to any particular lock — it is intended just to move the mechanical components of the cylinder in a more or less random way until the lock spontaneously opens. This only works on the simplest, cheapest locks. A pack of 10 jiggler keys is available for less than $4 on Amazon.

The investigator was able to open the lock in just about five seconds using what was in fact the simplest of his jiggler keys. He was then able to open the panel, which exposed:

- The power switch
- The USB port

- The modem port
- The printing mechanism

The investigator also noticed that there was no sensor to indicate when the faceplate was opened or closed, so even when the machine is powered on and running there was no possibility of logging the occasions when it was opened or closed.

Anyone who has a few seconds access to the WINVote machine can open the front panel. This obviously includes election officials, warehouse workers, and poll workers. And, if a voter hides the front of the machine with her body as she jimmies the lock, she may be able to open the panel without detection.

Once the panel is open, anyone with sufficient time and preparation could:

- Power the machine on or off. Powering off at the wrong moment may result in a corrupted file system or database;
- Install malicious software through the USB port. This includes malicious software which could modify vote counts arbitrarily with no logging or forensic evidence that it happened;
- Connect the machine to the Internet through the modem port. Connecting a voting machine to the Internet opens it to a host of threats, including remote login and the installation of malicious software, particularly because the WINVote runs a very early and extremely vulnerable version of Window XP; or
- Disable the print mechanism.

Recommendation:
Make A Crisis Communications Plan Before Your Website is Hacked

Given the scope of vulnerabilities inherent in the U.S. election system, it is vital that state and local election officials not only seek to prevent cyber attacks on their systems, but also plan how best to recover from an attack. One of the primary challenges in this new era of foreign propaganda is disseminating accurate information to constituents in a reliable manner. The following is a list of recommendations to prepare for an attack against an election results reporting website on Election Day. These recommendations are intended to ensure results are communicated in a way that engenders trust in the election results from voters. This list is tailored to specifically address a cyber attack on an election website but was largely sourced from the Local Government Association of England and Wales[10] who created these recommendations for any government crisis communications plan in response to a cyber attack. We would like to thank the Local Government Association of England and Wales for their thoughtful work on this important topic.

1. **Anticipate crisis conditions and create a crisis communications plan**
   Organizational leaders should anticipate what conditions might be created by a cyber attack on their systems, such as the publication of false election results on official websites, as happened in Ukraine,[11] or a Distributed Denial of Service (DDoS) attack that could shut down the site altogether, as happened to many U.S. banks in the Iranian attack[12] and create a plan for how to communicate with the public and other stakeholders under such conditions. This plan should be part of a local or state government's overall emergency planning. Effective crisis communications plans should include:

   - Who will be part of the crisis communications team
   - Timeline of when the crisis communications team should meet during the first hours, days, and weeks following a crisis
   - Who has ultimate authority for signing off on key messages
   - List of audiences who need to be reached during a crisis, including contact details
   - List of stakeholders to reach out to or work with during a crisis, including contact details
   - List of channels to be used to communicate messages, including multiple backup options
   - Copies of passwords needed to access official communication channels

   Needless to say, this crisis communications plan should be kept in hard copy in case of compromised systems.

2. **Prepare and practice**
   Designated crisis communications teams should practice their response processes to ensure the plan works smoothly and each team member knows his or her role during an emergency. In case of

[10] "Crisis Communications - Cyber Attack," Local Government Association, https://www.local.gov.uk/our-support/guidance-and-resources/comms-hub-communications-support/cyber-attack-crisis.
[11] Andy Greenberg, "How An Entire Nation Became Russia's Test Lab for Cyberwar, June 20, 2017, https://www.wired.com/st ory/russian-hackers-attack-ukraine/.
[12] Dustin Volz and Jim Finkle, "U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam," *Reuters*, March 24, 2016, https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF.

a cyber attack, team members should be aware of what dangers they can expect and how to report concerns about suspicious activity.

3. **Establish facts, communicate early and regularly**
   During a crisis situation, the crisis communications team should proactively communicate known facts as early as possible, rather than reacting to rumor and speculation. The team should also continually update the public and other stakeholders at regular intervals to remain in control of the messaging.

4. **Identify a spokesperson**
   Before a crisis event, organizational leaders should designate a senior member of the organization to act as spokesperson for the team in case of a crisis. This should be a designated team member who is not directly involved in solving the crisis, which would distract them from focusing on key messages and relaying information in a timely manner.

5. **Avoid email and website updates**
   If an organization is the target of a suspected or confirmed cyber attack, team members should stop using email and website messaging immediately.

6. **Embrace traditional channels**
   When digital communications platforms are compromised by a suspected or confirmed cyber attack, the designated spokesperson should utilize other communications channels to relay key messages, including holding telephone calls with local media, staging in-person press briefings, or utilizing telephone trees to share updates with staff members.

7. **Brief media outlets and elected officials**
   If a cyber attack takes place, the crisis communications team alert news media and elected officials that they may experience a surge in calls from the public. These stakeholders should also receive timely updates on the crisis so they can keep members of the public who contact them informed of the situation.

8. **Use personal devices if possible**
   If an organization's IT systems are compromised, employees may still have access to the organization's digital communications platforms, such as social media accounts, via their personal devices. The crisis communications team should keep hard copies of social media passwords available for this situation.

9. **Use partner and community networks**
   If an organization is targeted by a cyber attack, the crisis communications team should reach out to established partner organizations for help disseminating accurate, up-to-date information on their respective digital platforms. The crisis communications team should establish these relationships before a crisis occurs.

10. **Engage with IT and legal colleagues**
    Members of the crisis communications team should work closely with the organization's IT and legal team when preparing to brief the public on updates throughout the crisis. Particularly in the case of a cyber attack, technical details may be difficult to communicate clearly and understand in the appropriate technical and legal contexts.

11. Communicate with employees

In the midst of a crisis, an organization's leaders should share updates with staff members before communicating with the broader public. If staff members hear updates via social media or other channels before hearing it from their leadership team, it can damage trust within an organization and undermine efforts to control and mitigate the effects of the crisis.

12. Respond to the new normal

Following a crisis like a cyber attack, an organization's leaders should craft messages for stakeholders and the broader public that communicate the lessons learned from the crisis and how the organization is evolving to safeguard against such attacks in the future. Such messaging can repair trust in the organization and help other organizations protect themselves against future crises.

Conclusion

Over the last 26 years, DEF CON, and for the last two years, the Voting Village, have operated under two core principles:

1. **It is important to derive facts through reason and inquiry rather than blind faith.**

2. **When we discover new facts, it's important we share this information with the general public so individuals can decide how best to use the information.**

We did not make these principles up ourselves. Rather, these principles are the foundation of the Enlightenment, which has guided modern science to achieve the medical, engineering, and IT advances, among others, that underpin the modern world. Since these principles have largely guided the human race toward progress for the last 500 years, we plan to continue to follow them.

These principles matter most when we put them into practice. Therefore, it is relevant to ask what new facts all the poking and inquiring into our voting systems has identified since the Voting VIllage was established.

Among the dozens of vulnerabilities identified in the last two years, four key DEF CON Voting Village findings are grave and undeniable:

1. **Supply Chain Insecurity:** The voting machine parts supply chain is global and has essentially no security procedures to determine whether the machine parts are trustworthy or pre-hacked before the machine is assembled. Thus if an adversary compromised chips through the supply chain, they could hack whole classes of machines across the U.S., remotely, all at once.

2. **Remote Attacks Proven:** Despite insistence the fact that machines are "air gapped" from the Internet protects against all remote attacks, both DEF CON 25 and 26 found exploits to hack machines remotely, requiring physical access to the machine.

3. **Hacking Faster Than Voting:** This year DEF CON also demonstrated that while, on average, it takes about six minutes to vote, machines in at least 15 states can be hacked with a pen in two minutes. It is thus possible for someone to hack a machine while voting in a polling place on Election Day.

4. **Hacks Don't Get Fixed:** Finally, we discovered that even when vendors are told about serious flaws in machines by their customers, those flaws go unfixed.

These flaws are relevant and disturbing under the best circumstances. However, the fourth flaw suggests another reason for alarm - disclosing vulnerabilities does not seem to be enough to get them fixed, even years later. For example, the M650's lack of update authentication was noted in the 2007 EVEREST report, initiated by the Secretary of State of Ohio and reported to Election Systems & Software at the same time.[13]

[13] Pennsylvania State University, the University of Pennsylvania, and WebWise Security Inc, EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing. Compiled by Patrick McDaniel. By Matt Blaze and Giovanni Vigna. December 7, 2007. Accessed September 25, 2018. https://www.eac.gov/assets/1/28/EVEREST.pdf.

Hackers found the same design flaw in a current M650, eleven years later. As of 2018, the M650 was used in elections in 23 states.

The failure to fix existing, reported vulnerabilities and the disconnect between the reports of election security experts and the reactions of some election equipment vendors speaks directly to the reason Voting Village was created. The Voting Village aims to increase access to election security knowledge in order to better protect American democracy and the electoral system. We believe that knowing the risks involved in how America votes is always better than sticking our heads in the sand. Although we have redacted some information from this report, it is a realistic, if pessimistic, view of how easy it is for individuals to exploit bad design and sidestep election protections. We hope that it will move the United States towards action.

Next Steps:

1. **Congress Must Act:** The problems outlined in this report are not simply election administration flaws that need to be fixed for efficiency's sake, but rather serious risks to our critical infrastructure and thus national security. As our nation's security is the responsibility of the federal government, Congress needs to codify basic security standards like those developed by local election officials.

2. **Congress Must Fund Election Security:** National defense is not the role of state and local government. Further, no state or local government will ever be able to raise enough capital to defend itself from a determined nation state. Thus, having codified the basic security standards developed by local election officials above, Congress must finance the implementation of these security standards.

3. **Create a Crisis Communications Plan Now:** State and local government election results web pages are, by their very nature, the most insecure component of our election infrastructure. Using the crisis communications plan listed in this document, election administration teams can plan for this attack in advance so they are not scrambling for solutions if an attack happens on Election Night.

4. **National Security Leaders Must Act:** While many local election officials have worked tirelessly to advocate for Congress to act and fund robust security practices, it's not enough. National security leaders must also remind Congress daily of the gravity of this threat and national security implications. It is the responsibility of both current and former national security leaders to ensure Congress does not myopically view these issues as election administration issues but rather the critical national security issues they are.

End Notes

By: Noah Praetz, Director of Elections, Cook County, Illinois

There is nothing more important to election officials than security. Period. Security yields trust and participation. We have been securing votes and voter records for a long time. The threat environment has changed dramatically, we accept the admonitions of our intelligence community, and we understand the significantly increased likelihood of a successful cyber-attack on the election infrastructure. The Secretaries of State, State Election Directors, and local election officials are committed to ensuring that the election results we release are trusted and true.

In this new environment, and in light of existential threats to American faith in democracy, election officials will marshal all available resources, and work with all possible partners, in defense of elections. Those of us who manage elections, and our vendor community, have long-standing partnerships with private security researchers. However, those partnerships are no longer enough; we are building new partnerships with a broader security research community. Building these new partnerships, with organizations like DEF CON, has proven challenging for some in our community over the past two years. Maturing this partnership will require mutual trust and appreciation of each other's roles, responsibilities, and motives. Ultimately, a successful relationship will be forged, out of necessity.

Election officials recognize that today's cyber threat environment necessitates access to the highest levels of security expertise. This talent is expensive. Therefore, we must accept that our new partners are indispensable but bring stylistic and cultural differences that we'll need to learn to manage and accept. Our new partners must accept that the security and resiliency of the election infrastructure and process demands a unique level of sensitivity and care. When other industries are alerted to issues, there are patches at hand or in a pipeline. Frequently, election technology is frozen in time by federal and state certifications that make immediate fixes impossible.

This change in attitude and posture, from election officials and security researchers alike, is a dramatic one. This cultural difference is most pronounced when the public messaging over the same information sets about election security are diametrically opposed. In the security community, exploitable vulnerabilities are a binary fact that should be publicly disclosed and remediated with updated technology as soon as possible. The election official community sees the same vulnerabilities and recognize them as something to be mitigated with physical controls and managed with audits immediately and then remediated as soon as the technology and funding is available.

Despite the differences, the goals are the same for election officials and security researchers. It's the requirement to operate elections in the time between vulnerability disclosure and vulnerability fix, and to provide trust in the process simultaneously, that causes consternation and tension.

Given the capability and intent of American adversaries, whether nation states, groups, or individuals, election officials' failure to capitalize on the expertise of the broader security research community is no longer acceptable. Likewise, given the dire need for the expertise of the security community, failure of that community to appreciate and respond to sensitivities about the sanctity and security of American elections is also no longer acceptable. We must make this relationship work.

Our elected Clerk in Cook County, Illinois, David Orr, understood this two years ago and decided to seek

help where available, to interface with experts where possible, and to be available to well-meaning Americans focused on election security.

One of our first avenues of engagement was with the organizers of the Voting Village at DEF CON in the spring of 2017. We offered consulting services on what an election office backend network might reasonably look like to ensure that the conclusions reached by the security researchers, and by extension the lessons learned by election administrators, were grounded in reality. It does little good for the community of researchers or election officials if the conclusions drawn in the reports can be readily dispelled, either in fact or in art.

After DEF CON released its report in 2017 we drafted a white paper that laid out priorities for funders like federal, state and local governments, and for election officials. It was built around an election security framework, Defend, Detect, Recover. Do everything possible to defend the myriad digital systems relied upon to run modern elections. Recognize perfect defense may not be possible all the time. Ensure that defensive shortfalls can be detected. And that business continuity, or recovery, can be established such that our elections can be run even in the event of successful cyber-attacks.

Between 2017 and 2018 the Voting Village dramatically increased their focus and shifted their research and training to more vulnerable areas that are more likely to be attacked, like emailed ballots, voter registration databases, election officials' computer networks, and informational or election night results webpages. Some election officials consulted with the organizers in some of these areas. Where there was consultation, like on the computer network and voter registration databases, the resulting research and training is more valuable. Where there was less election official participation, like on the webpages, the research was less valuable. And while the headlines about 11-year-olds hacking website were overstated, and frustrating given the websites were not actual replicas, the DEF CON Voting Village has done as much to raise awareness about our needs for resources as we have been able to do for ourselves. For that we owe some acknowledgement and credit, even as some of us have been forced to reassure our voters that not everything they have read about applies. I believe that the leaders and participants in the Voting Village and of the DEF CON project broadly, are talented committed Americans dedicated to ensuring that election officials know what they are dealing with from a product standpoint, and that we are supported in our efforts to raise the funds necessary to ensure the highest possible state of readiness.

Simultaneous to the activities of the security research community, the U.S. Department of Homeland Security created a set of councils to help drive their investments in election security. They rely on election officials at all levels and on the vendor community. I co-chair the Government Coordinating Council. In that role I have sought to bring visibility to that fact that nearly the entire profile of election security is borne by the 8,800 local election officials in this country; and though we locals find overheated rhetoric about election security difficult and angering, our real and present needs to access security expertise supersedes those frustrations.

In closing, I'll repeat, there is nothing more important to election officials than security. The security researcher community, like those who managed and attended the Voting Village at DEF CON, also care greatly about election security. We need these security researchers on our team; and we also need them to be as careful and responsible with their disclosures and language as possible. We won't always agree and there will be very uncomfortable times. But I see a strong partnership moving forward as both communities learn to work together and appreciate each other's needs and perspectives.

Acknowledgements

A number of individuals and organizations contributed to the Voting Village and to this report. A special thanks to:

- Organizers, subject-matter-experts and other visionaries who turned the Voting Village concept into a reality and helped to author this report;
- KIG and CyberBit, for providing use of the KIG CyberRange;
- Speakers who contributed to the Voting Village discussions, including representatives from the U.S. Department of Homeland Security, Free & Fair, Verified Voting, and the University of Chicago Harris Cyber Policy Initiative; and
- The Michael and Paula Rantz Foundation, for their generous support of this work.

APPENDIX #1: Partial List of Attending Individuals & Organizations

Representatives attended the event from a variety of organizations including:

Voting Village Speakers

- **Diego Aranha**, Assistant Professor - Department of Engineering, Aarhus University
- **Matthew Bernhard,** PhD Candidate - Computer Science, University of Michigan; Data Science Consultant, Verified Voting Foundation
- **Matt Blaze**, Cryptographer & Associate Professor of Computer & Information Science, University of Pennsylvania
- **Jake Braun**, Executive Director, University of Chicago Harris Cyber Policy Initiative; CEO, Cambridge Global Advisors
- **Alex Halderman**, Professor of Computer Science & Engineering, University of Michigan; Verified Voting Technology Fellow
- **Jason Hill,** Director, Red Team Lead, Department of Homeland Security
- **Harri Hursti,** Co-Founder, Nordic Innovation Labs
- **Rob Karas**, Director, National Cybersecurity Assessments and Technical Services (NCATS), Department of Homeland Security
- **Neal Kelley**, Chief of Elections, Registrar of Voters, Orange County, California
- **Joe Kiniry,** Principal Scientist, Galois; Principled CEO and Chief Scientist, Free & Fair
- **Margaret MacAlpine**, Founding Partner, Nordic Innovation Labs
- **Jeanette Manfra**, National Protection and Programs Directorate (NPPD) Assistant Secretary for the Office of Cybersecurity and Communications (CS&C), DHS
- **Alejandro Mayorkas,** Partner, WilmerHale; former Deputy Secretary, U.S. Department of Homeland Security
- **Amber McReynolds**, Executive Director, National Vote at Home Coalition; former Director of Elections, City and County of Denver, Colorado
- **Alex Padilla**, Secretary of State, California
- **Noah Praetz**, Director of Elections, Cook County, Illinois
- **David Sanger**, National Security Correspondent and Senior Writer, *The New York Times*; Author, *The Perfect Weapon*

Other Key Stakeholders in Attendance

- **Barb Byrum**, County Clerk, Ingham County, Michigan
- **Rob Joyce**, Senior Advisor for Cyber Security Strategy to the Director of the National Security Agency (NSA)
- **Brian Markus**, Co-Founder and CEO, Aries Security
- **John Odum**, City Clerk, Montpelier, Vermont
- **Nico Sell**, CEO, Wickr; Founder, r00tz Asylum

APPENDIX #2: Biographical Information: Voting Village Speakers

Diego Aranha, Assistant Professor - Department of Engineering, Aarhus University
Diego F. Aranha is an Assistant Professor in the Department of Engineering at Aarhus University. He was previously an Assistant Professor at the University of Brasília and the University of Campinas. His professional experience is in Applied Cryptography and Computer Security, with a special interest in the efficient implementation of cryptographic algorithms and security analysis of real-world systems, and includes coordinating two teams of independent researchers capable of detecting and exploring vulnerabilities in the software of the Brazilian voting machine during controlled tests organized by the national electoral authority. He received the Google Latin America Research Award twice for research on privacy, and the MIT TechReview's Innovators Under 35 Brazil Award for his work in electronic voting.

Matthew Bernhard, PhD Candidate - Computer Science, University of Michigan; Data Science Consultant, Verified Voting Foundation
Matt Bernhard is a third year computer science Ph.D. candidate at the University of Michigan with Professor Alex Halderman. He graduated with a B.A. in Computer Science from Rice University in 2015, where he worked with Professor Dan Wallach on STAR-Vote. He has also spent time at Microsoft Research working on remote attestation and security protocols involving secure kiosks with Josh Benaloh, and at Cloudflare working on certificate transparency and SSL/TLS features. His research interests focus on the broad social implications of technology and privacy, delving into computer security, cryptography, networks, usability, censorship, systems, and voting technology.

Matt Blaze, Cryptographer & Associate Professor of Computer & Information Science, University of Pennsylvania
Matt Blaze is a professor at the University of Pennsylvania, where he directs the Distributed Systems Lab and conducts research in security, privacy, surveillance, cryptography, scale, and the relationship between technology and public policy. His work has included the discovery of fundamental flaws in the Clipper chip and other surveillance systems, foundational work in network security, file encryption, trust management and two way radio security, and security evaluations of major electronic voting systems used in the US.

Jake Braun, Executive Director, University of Chicago Harris Cyber Policy Initiative
Jake Braun is Executive Director of the University of Chicago Harris Cyber Policy Initiative (CPI), CEO of Cambridge Global Advisors (CGA), and Co-Founder of the DEF CON Voting Village. Previously, he was the White House Liaison to the Department of Homeland Security (DHS). He has twenty years experience in national security and strategic communications initiatives.

Alex Halderman, Professor of Computer Science & Engineering, University of Michigan; Verified Voting Technology Fellow
J. Alex Halderman is Professor of Computer Science & Engineering at the University of Michigan and a Verified Voting Technology Fellow. His research spans computer and network security, applied cryptography, security measurement, censorship resistance, and electronic voting, as well as the interaction of technology with politics and international affairs. Halderman helped discover the cold boot attack and the TLS Logjam and DROWN vulnerabilities, and he co-founded the ZMap Project, Censys.io, and Let's Encrypt. A noted expert in election cybersecurity, he has performed numerous evaluations of real-world voting systems, both in the U.S. and around the world. After the 2016 U.S. presidential election, he advised recount initiatives in Michigan, Wisconsin, and Pennsylvania in an effort to help detect and deter

cyber attacks, and in 2017 he testified to the U.S. Senate intelligence committee about cybersecurity threats to election infrastructure. He has been named by Popular Science as one of the "brightest young minds reshaping science, engineering, and the world."

Jason Hill, Director, Red Team Lead, Department of Homeland Security
Jason Hill came to the Department of Homeland Security (DHS) in 2013 to help create the Nation's Red Team. Hill has over 24 years in the Information Security field and over 22 years in the Army National Guard within the cyber security domain. Hill serves as the Deputy Chief of the National Cybersecurity Assessments and Technical Services (NCATS) Risk Evaluation team and as the Chief of the Red Team conducting Red Team Assessments for Federal Government customers. Prior to DHS, Hill served as a Red Team instructor to military and Federal Government employees. He holds a B.S. in Computer Information Systems and several industry certificates.

Harri Hursti, Co-Founder, Nordic Innovation Labs
Harri Hursti is among the world's leading authority in data and election voting security, critical infrastructure, and network security systems. Beginning his career as one of the minds behind the first commercial, public email and online forum system in Scandinavia, he went on to cofound EUnet-Finland. Hursti has authored many studies on election security and vulnerability in both academic and corporate publications. He worked for Black Box Voting where he performed voting machine hacking tests, which became known as the Hursti Hacks. These tests were filmed and later turned into the acclaimed HBO documentary *Hacking Democracy.*

Rob Karas, Director, National Cybersecurity Assessments and Technical Services (NCATS), Department of Homeland Security
A certified information systems security professional with over 17 years of experience in information security in the commercial and federal sectors, Karas has extensive experience conducting risk and security assessments and managing information security programs. In his current role as Director, Karas manages the NCATS team at DHS and provides cybersecurity services to Federal Agencies, State, Local, Tribal, and Territorial governments. He is responsible for creating and identifying new services and developing the NCATS program into the civilian governments leading security services provider. Prior to joining DHS, Karas worked in the private sector for 12 years developing security operations. He holds a Bachelor of Science in Information Management from James Mason University.

Neal Kelley, Chief of Elections, Registrar of Voters, Orange County, California
Neal Kelley is Registrar of Voters for Orange County, California, the fifth largest voting jurisdiction in the United States. As the Chief Election Official, Kelley has led the Registrar of Voters' office through the largest cycle of elections in the County's 129-year history. He has been the recipient of numerous state and national awards for election administration and was recently awarded the "Public Official of the Year" award by the National Association of County Recorders, Election Officials and Clerks.

Kelley is an appointee of the U.S. Department of Homeland Security, Government Coordinating Council (GCC), which helps to oversee the protection of the nation's election infrastructure, Kelley holds an M.B.A. from the University of Southern California and a Bachelor of Science from the University of Redlands.

Joe Kiniry, Principal Scientist, Galois; Principled CEO and Chief Scientist, Free & Fair
Dr. Joseph Kiniry is a Principal Scientist at Galois and the Principled CEO and Chief Scientist of Free & Fair. Previously, he was a Full Professor at the Technical University of Denmark where he was the Head of the Software Engineering section. Since the early 2000s he has held permanent positions at four universities in

Denmark, Ireland, and The Netherlands. Dr. Kiniry has extensive experience in formal methods, high-assurance software and hardware engineering, foundations of computer science and mathematics, and information security.

Margaret MacAlpine, Founding Partner, Nordic Innovation Labs
Margaret MacAlpine is a system testing technologist and election auditing specialist. Her work includes projects with electronic testing of voting registration systems, election security, and election fraud. MacAlpine is a specialized technologist in testing and performing risk limiting and transitive audits on election results. Before joining Nordic Innovation Labs, MacAlpine served as an advisor for the office of the Secretary of State of California, specifically with the Risk Limiting Audit Pilot Program where she developed her expertise on the use of high-speed scanners for conducting post-election audits. In partnership with the University of Michigan, MacAlpine contributed to the research of security analysis and the Estonian internet voting system. MacAlpine earned her Bachelor of Arts from Trinity College in Hartford, Connecticut.

Jeanette Manfra, National Protection and Programs Directorate (NPPD) Assistant Secretary for the Office of Cybersecurity and Communications (CS&C), DHS
Ms. Manfra leads the Department of Homeland Security (DHS) mission of strengthening the security and resilience of the nation's critical infrastructure. Prior to this position, Ms. Manfra served as Acting Deputy Under Secretary for Cybersecurity and Director for Strategy, Policy, and Plans for the NPPD.

Previously, Ms. Manfra served as Senior Counselor for Cybersecurity to the Secretary of Homeland Security and Director for Critical Infrastructure Cybersecurity on the National Security Council staff at the White House. At DHS, she held multiple positions in the Office of Cybersecurity and Communications, including advisor for the Assistant Secretary for Cybersecurity and Communications and Deputy Director, Office of Emergency Communications, during which time she led the Department’s efforts in establishing the Nationwide Public Safety Broadband Network.

Before joining DHS, Jeanette served in the U.S. Army as a communications specialist and a Military Intelligence Officer.

Alejandro Mayorkas, Partner, WilmerHale; former Deputy Secretary, U.S. Department of Homeland Security
Alejandro Mayorkas represents clients in civil litigation and internal investigations, and augments the firm's formidable strengths in strategic counseling, crisis management and national security, with a particular focus on cybersecurity.

Before joining WilmerHale, Mayorkas served as Deputy Secretary of Homeland Security, where he managed some of the most complex and critical responsibilities of government, including preventing and responding to terrorist attacks on US soil, enhancing both the government's and the private sector's cybersecurity, enforcing the nation's immigration laws, facilitating lawful trade and travel, and helping stricken communities recover from disasters. For his service as Deputy Secretary of Homeland Security, Mayorkas received the Department's Distinguished Service Award, its highest civilian honor; the US Coast Guard's Distinguished Service Award; a special commendation from the National Security Agency for his achievements in national security and, specifically, cybersecurity; and numerous additional awards and commendations.

As Deputy Secretary, Mayorkas was the Obama Administration's highest ranking Cuban American and was named to Latino Leaders' list of the nation's most influential Latinos. In 2008, The National Law Journal recognized him as one of the "50 Most Influential Minority Lawyers in America."

Prior to becoming Deputy Secretary, Mayorkas served as Director of US Citizenship and Immigration Services, the federal agency that administers the largest legal immigration system in the world.

From 1998 to 2001, Mayorkas served as the US Attorney for the Central District of California, where he oversaw prosecutions of national significance, including the investigation and prosecution of financial fraud, violations of the Foreign Corrupt Practices Act (FCPA), public corruption, cybercrime, international money laundering, and immigration fraud. He was promoted to the Senate-confirmed position of US Attorney after having served for nearly nine years as an Assistant US Attorney specializing in the prosecution of financial fraud.

After leaving the US Attorney's Office, Mayorkas developed a civil litigation and internal investigations practice representing a wide range of corporate clients across the country.

Mayorkas serves as Chairman of the US Chamber of Commerce's Cyber Leadership Council. The Cyber Leadership Council serves as a forum for businesses to openly discuss cybersecurity policy and practices, direct Chamber advocacy and education efforts, and serve as a key voice of industry for dialogue with policymakers.

Amber McReynolds, Director of Elections, City and County of Denver, Colorado
A subject matter expert on elections, Amber McReynolds has been involved in the election's office thirteen years and has been focused on improving the election experience for the people of Denver. McReynolds has played a critical role in modernizing the election model in Colorado and has taken steps to promote innovation and election efficiency in Denver. McReynolds is currently preparing to step into the executive director role of a voter-based nonprofit, National Vote at Home Institute and Coalition. McReynolds holds a Master of Science in Comparative Politics from the London School of Economics and a Bachelor of Science from the University of Illinois.

Alex Padilla, Secretary of State, California
Alex Padilla was sworn in as California Secretary of State on January 5, 2015. He is committed to modernizing the office, increasing voter registration and participation, and strengthening voting rights.

Padilla previously served in the California State Senate (2006-2014) where he chaired the Committee on Energy, Utilities, and Communications. As chair, he shepherded legislation to combat climate change and create a greener and more sustainable economy. He pursued an ambitious agenda in the areas of renewable energy, energy efficiency, smart grid, and broadband deployment. In 1999, at the age of 26, Padilla was elected to the Los Angeles City Council to represent the same east San Fernando Valley community where he grew up. In 2001, his colleagues elected him to the first of three terms as Council President, becoming the youngest member and the first Latino to serve in this capacity.

Noah Praetz, Director of Elections, Cook County, Illinois
Responsible for all matters of election administration in one of the largest jurisdictions in the country, Praetz has extensive experience in election day management, election security, and voter registration modernization. Praetz also serves on the executive committee of the Government Coordinating Council

where he represents local election officials. Additionally, he serves as co-chair of the Election Center Cyber Security Committee and is a member of the International Association of Government Officials and the Illinois Association of County Clerks and Recorders. Praetz publishes articles on cybersecurity, Election Day administration and referred law in Illinois.

Praetz began his career doing data entry prior to the 2000 presidential elections. He worked his way through the ranks in the elections department before taking the position of Deputy Director and then advancing to his current position as Director. Praetz holds a Juris Doctor from DePaul University College of Law.

David Sanger, National Security Correspondent and Senior Writer, *The New York Times*; Author, *The Perfect Weapon*

David E. Sanger is a national security correspondent and a *Times* senior writer. In a 36-year reporting career for *The New York Times,* he has been on three teams that have won Pulitzer Prizes, most recently in 2017 for international reporting. His newest book, "The Perfect Weapon: War, Sabotage and Fear in the Cyber Age,'' examines the emergence of cyberconflict as the primary way large and small states are competing and undercutting each other, changing the nature of global power.

He is also the author of two Times best sellers on foreign policy and national security: "The Inheritance: The World Obama Confronts and the Challenges to American Power," published in 2009, and "Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power," published in 2012. For The Times, Sanger has served as Tokyo bureau chief, Washington economic correspondent, White House correspondent during the Clinton and Bush administrations, and chief Washington correspondent.

Sanger spent six years in Tokyo, writing about the emergence of Japan as a major American competitor, and then the country's humbling recession. He wrote many of the first articles about North Korea's emerging nuclear weapons program.

Returning to Washington, Sanger turned to a wide range of diplomatic and national security issues, especially issues of nuclear proliferation and the rise of cyberconflict among nations. In reporting for The Times and "Confront and Conceal," he revealed the story of Olympic Games, the codename for the most sophisticated cyber attack in history, the American-Israeli effort to sabotage Iran's nuclear program with the Stuxnet worm. His journalistic pursuit of the origins of Stuxnet became the subject of the documentary "Zero Days," which made the short list of Academy Award documentaries in 2016. With his Times colleague Bill Broad, he also described, in early 2017, a parallel cyber effort against North Korea.

Sanger was a leading member of the team that investigated the causes of the Challenger disaster in 1986, which was awarded a Pulitzer in national reporting the following year. A second Pulitzer, in 1999, was awarded to a team that investigated the struggles within the Clinton administration over controlling technology exports to China. He has also won the Weintal Prize for diplomatic reporting for his coverage of the Iraq and Korea crises, the Aldo Beckman prize for coverage of the presidency, and, in two separate years, the Merriman Smith Memorial Award, for coverage of national security issues. "Nuclear Jihad," the documentary that Sanger reported for Discovery/Times Television, won the duPont-Columbia Award for its explanation of the workings of the A. Q. Khan nuclear proliferation network. That coverage was also a finalist for a Pulitzer.

A 1982 graduate of Harvard College, Sanger was the first senior fellow in The Press and National Security at the Belfer Center for Science and International Affairs at Harvard. With Graham T. Allison Jr., he co-teaches

Central Challenges in American National Security, Strategy and the Press at the Kennedy School of Government.

Carsten Schurmann, Professor of Computer Science at IT University of Copenhagen
With 10 years of experience conducting research in elections, Carsten Schuermann is an expert in election security. Schuermann has written over academic 60 papers, contributed to books, and hacked at DEF CON 2017 the WinVote voting machine shortly after the Voting Machine Voting village opened. Schuermann is a member of the computer science faculty at IT University of Copenhagen and leads the Center for Information Security Research. He has worked with the Carter Center, USA, Council of Europe, Venice Commission, and International IDEA (Sweden).

Before, joining the University of Copenhagen, Schuermann was a member of the Computer Science Department at Yale University. Schuermann holds a Ph.D. degree in Computer Science from Carnegie Mellon University, and a German Master in Computer Science from University of Karlsruhe.

APPENDIX #3: Don't Take Our Word For It

The DEF CON Voting Village provides vital information about vulnerabilities in the U.S. election system to state and local election officials in order to better safeguard the foundations of our democracy. Cross-sector collaboration is critical in overcoming the challenges posed by cybersecurity threats. But you don't have to take our word for it.

Senator James Lankford, Oklahoma
December 21, 2017
Press Release[14]

> "Safe and free elections run by individual states are at the core of our national identity…. During the 2016 elections, Russia tried to interfere in our elections. Although they didn't change actual votes or alter the outcome, their efforts were an attack on our democracy. It is imperative that we strengthen our election systems and give the states the tools they need to protect themselves and the integrity of voters against the possibility of foreign interference. In this new digital age, we should ensure the states have the resources they need to protect our election infrastructure."

Senator Amy Klobuchar, Minnesota
December 19, 2017
Letter to Department of Homeland Security Secretary Kirstjen Nielsen[15]

> "We must … provide states with resources, best practices and manpower to help combat attacks and update voting technology. State and local officials are on the front lines of our democratic process. It is wrong to leave them defenseless against sophisticated cyber hackers backed by the Kremlin and other adversaries."

Senator Bernie Sanders, Vermont
August 13, 2018
Facebook

> "This November may be the most important election of our lifetimes, and we must do everything in our power to protect our democratic processes. Congress must move aggressively to protect our election systems from interference by Russia or any foreign power, and work closely with our democratic partners around the world to do the same."

Senator Kamala Harris, California
Senator Mark Warner, Virginia
Senator James Lankford, Oklahoma
Senator Susan Collins, Maine
August 22, 2018

---

[14] James Lankford, United States Senator for Oklahoma. "Senators Lankford, Klobuchar, Harris, Collins, Heinrich and Graham Introduce Election Security Bill." News release, December 21, 2017. Accessed September 26, 2018. https://www.lankford.senate.gov/news/press-releases/senators-lankford-klobuchar-harris-collins-heinrich-and-graham-introduce-election-security-bill.

[15] Amy Klobuchar, United States Senator for Minnesota. "Department of Homeland Security Secretary Nielsen Begins Tenure, Klobuchar, Lankford Urge Making Election Cybersecurity a Top Priority." News release, December 19, 2017. Accessed September 26, 2018. https://www.klobuchar.senate.gov/public/index.cfm/news-releases?ID=B3961145-FBA8-4B71-BA36-0EB4FAB29C0E.

Letter to Tom Burt, President, Election Systems & Software (ES&S)[16]

> "The reality of these unprecedented security risks was on full display at the DEF CON cybersecurity conference, where researchers at the "Voting Village" successfully probed a variety of electronic equipment used to administer elections. We are disheartened that ES&S chose to dismiss these demonstrations as unrealistic and that your company is not supportive of independent testing. We believe that independent testing is one of the most effective ways to understand and address potential cybersecurity risks."

Congresswoman Jackie Speier, 14th District, California

August 13, 2018

Twitter[17]

> "If an 11 yr old can change votes on a FL election system, what can a nefarious, trained Russian spy do? There are only 7 companies making election machines that contract with our states and counties, and these companies refuse to let anyone test their software! @VotingVillageDC"

Congresswoman Tulsi Gabbard, 2nd District, Hawaii

August 14, 2018

Press Release[18]

> "Kids being able to hack into our election infrastructure in mere minutes highlights the severe vulnerabilities in our election infrastructure that threaten our American democracy. These vulnerabilities erode voter confidence and expose our election outcomes to manipulation. With the 2018 general election quickly approaching, Congress must act now to pass my Securing America's Elections Act, and work with the states to safeguard our electoral infrastructure, ensuring that each and every American vote is counted faithfully and accurately."

Jeanette Manfra, National Protection and Programs Directorate (NPPD) Assistant Secretary for the Office of Cybersecurity and Communications (CS&C), Department of Homeland Security

August 10, 2018

Panel at DEF CON Voting Village[19]

> "We'd love it if you [DEF CON attendees] worked for us. We'd love it if you worked with us."

Secretary of State Alex Padilla, California

August 10, 2018

Panel at DEF CON Voting Village[20]

> "While I thank the United States Congress for appropriating $340 million last month, let me be abundantly clear, we need more resources. All the things that we know we have to do, all the things

---

[16]Kamala D. Harris, Mark R. Warner, Susan M. Collins, and James Lankford to Tom Burt, President & Chief Executive Officer, Election Systems & Software, LLC. August 22, 2018. In Kamala Harris, U.S. Senator for California. August 22, 2018. Accessed September 26, 2018. https://www.harris.senate.gov/imo/media/doc/August 22 2018 - Letter to ESS.pdf.

[17] Speier, Jackie. Twitter Post. August 13, 2018, 2:49 PM. https://twitter.com/RepSpeier/status/1029122674801500160.

[18] Congresswoman Tulsi Gabbard, Hawaii's 2nd District. "Rep. Tulsi Gabbard on Vulnerability of US Election Systems Exposed at DEFCON." News release, August 14, 2018. Accessed September 26, 2018. https://gabbard.house.gov/news/press-releases/rep-tulsi-gabbard-vulnerability-us-election-systems-exposed-defcon

[19] Ng, Alfred. "US Officials Hope Hackers at Defcon Find More Voting Machine Problems." CNET. August 10, 2018. Accessed September 27, 2018. https://www.cnet.com/news/us-officials-hope-hackers-at-defcon-find-more-voting-machine-problems/.

[20] Hay Newman, Lily. "At DEFCON, the Biggest Election Threat Is Lack of Funding." WIRED. August 10, 2018. Accessed September 27, 2018. https://www.wired.com/story/defcon-election-threat-funding/.

that I'm going to learn and observe when I go down to the Village after this panel, to implement and act on all of these findings, recommendations, and discoveries we need official resources."

Secretary of State Jay Ashcroft, Missouri
August 14, 2018
KRCG[21]

"I want to work with them [DEF CON Voting Village] to make examples that are real world, that actually reflect what's actually happening in the states…. All those different points of views and ways of life and background, they help different individuals to see things that other people might miss."

Joel Miller, Linn County Auditor and Commissioner of Elections, Iowa
August 13, 2018
Blog post[22]

"At a recent Iowa State Association of County Auditors (ISACA) meeting in Iowa City, I heard officials from the Iowa Secretary of State's Office (SoS) discounting the value of any news or reports coming out of the Voting Machine Hacking Village at DEF CON® 26. Contrary to what the SoS said, I found the opposite. Every person I met seemed interested in elections, interested in the equipment we use, and interested in showing us the vulnerabilities of the equipment we use with an unexpected twist. That twist: What can I do to help election officials fix the problems?"

John Odum, Montpelier City Clerk, Vermont
July 19, 2018
GOVERNING[23]

"Too many election administrators are putting their faith in cybersecurity tools that by themselves don't provide nearly the level of security they need."

Joseph Holland, Santa Barbara County Registrar of Voters, California
County of Santa Barbara website[24]

"Attended DefCon 2017 (annual hacking conference) to observe their first ever Voting Systems Hacking Village. This was quite informative as it led to many ideas about how an election could be disrupted, including various social engineering attacks. This has led to internal discussions on how to mitigate these disruptions."

Amber McReynolds, Executive Director, National Vote at Home Institute and Coalition
August 14, 2018
Twitter[25]

---

[21] Lee, Kyreon. "Secretary of State Ashcroft Working toward Maintaining a Secure Election System." KRCG. August 14, 2018. Accessed September 27, 2018. https://krcgtv.com/news/local/secretary-of-state-ashcroft-working-toward-maintaining-a-secure-election-system.
[22] Miller, Joel. "DEF CON: A Confirmation about the State of Elections in Iowa." JoelMiller.us (blog), August 14, 2018. Accessed September 26, 2018. https://lcauditor.wordpress.com/2018/08/13/def-con-a-confirmation-about-the-state-of-elections-in-iowa/.
[23] http://www.governing.com/gov-institute/voices/col-election-security-use-training-tools-penetration-testing.html
[24] "Cyber Security - Frequently Asked Questions." County of Santa Barbara. Accessed September 27, 2018. https://countyofsb.org/care/elections/about/cyber-security.sbc.
[25] McReynolds, Amber. Twitter Post. August 14, 2018, 12:59 PM. https://twitter.com/AmberMcReynolds/status/1029457487051649024.

"Thanks @D_Hawk & @washingtonpost for covering #Defcon2018 ~ Improving the security of our #election systems requires commitment, collaboration, coordination, and communication. Continuous improvement is paramount! #DenverVotes"

Ashley Dittus, Democratic Commissioner, Ulster County Board of Elections, New York
August 24, 2018
Email to DEF CON Voting Village

"Thank you for the work you are doing to highlight this issue."

Cassandra Suettinger, Village Clerk/Treasurer, Village of McFarland, Wisconsin
August 27, 2018
Email to DEF CON Voting Village

"We are willing to take all the help we can get in securing our elections. While the hackers at DEF CON may not have all the answers, we are eager to learn about any vulnerabilities or security flaws that we can address and mitigate."

APPENDIX #4: Firewall Democracy: Best Practices for Securing America's Vulnerable Voting Infrastructure

FEBRUARY 2018

Firewall Democracy: Best Practices for Securing America's Vulnerable Voting Infrastructure

A secure vote forms the bedrock of our American democracy. Yet the lessons of 2016 made clear that nefarious actors possess the cyber capabilities to meddle in elections and undermine voters' faith.

Defending democracy is not a responsibility limited to any political party. This is an American challenge requiring a united effort to prepare for the 2018 elections and beyond.

Influenced by a host of cyber, national security, and election experts, this compilation offers 12 of the most widely-embraced best practices for securing U.S. election infrastructure.

PRODUCED IN PARTNERSHIP WITH

Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

DEFCON

Overview:
Cyber Threats & Challenges To Our Democracy

In 2016, Russia – a foreign adversary – led a campaign to infiltrate voter databases in at least in 21 U.S. states, possibly more. As that intelligence comes to light, it reiterates decades of expert warnings that, beyond Russia, many hostile actors have the cyber capability to tamper with our election infrastructure, perhaps best defined as a "patchwork" of outdated, aging voting equipment, registration databases, and networks that vary by state.

The ability to address the vulnerabilities in our elections is further complicated by the multiplicity of stakeholders charged with their protection. Voting systems are under the constitutional and administrative control of 50 states and thousands of local voting jurisdictions, many of which are under-resourced when it comes to cybersecurity. Yet election security is now firmly a national security matter, necessitating an evolving role for the federal government, particularly agencies like the U.S. Department of Homeland Security (DHS).

In short, firewalling democracy for 2018 and beyond will require significant coordination and funding at all levels – local, state, and federal – and action must come urgently.

> "Russia perceives its past efforts as successful and views the 2018 U.S. midterm elections as a potential target for Russian influence operations."
> *-Dan Coats,*
> *Director of National Intelligence*

> "Russia's activities in the 2016 election constituted the high-water mark of their long running efforts to disrupt and influence our elections. They must be congratulating themselves for having exceeded their wildest expectations with a minimal expenditure of resource. And I believe they are now emboldened to continue such activities in the future…"
> *-James Clapper,*
> *Former Director of National Intelligence*

Best Practices:
12 Action Items For Election Security

As the 2018 elections approach, this list of widely-accepted best practices from a variety of sources outlines **12 action items** to secure our elections.

Safeguard Voting Equipment

- Implement **universal use of paper ballots**, marked by hand and read by optical scanner, ensuring a voter-verified paper audit trail (VVPAT).
- **Phase out touch-screen voting machines** – especially the most vulnerable direct-recording electronic (DRE) devices
- **Update pollbooks** used to check-in voters.
- Verify voting results by requiring election officials to conduct **"Risk-Limiting Audits" (RLAs)**, a statistical post-election audit before certification of final results.

Protect Voting Networks & Databases

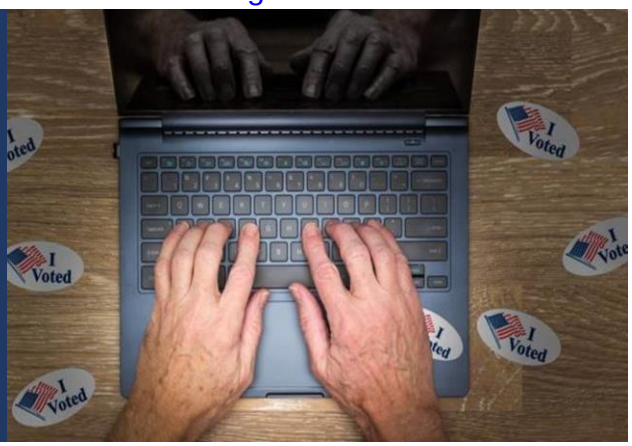
- **Secure voting infrastructure, especially voter registration databases**, using time-tested cyber hygiene tools such as the CIS "20 Critical Security Controls" or NIST's Cybersecurity Framework.
- **Call upon outside experts** to conduct cyber assessments – DHS, white-hat hackers, cybersecurity vendors and security researchers – where needed.
- **Provide resources and training** to state and local election leaders for cyber maintenance and on-going monitoring.
- **Promote information-sharing** on cyber threats and incidents in and across the entire voting industry.

Coordinate with Stakeholders

- **Appropriate federal funding** to states to implement infrastructure upgrades, audits, and cyber hygiene measures.
- **Establish clear channels for coordination** between local, state, and federal agencies, including real-time sharing of threat and intelligence information.
- Maintain DHS's **designation of elections as a Critical Infrastructure Subsector.**
- **Require DHS to institute a pre-election threat assessment plan** to bolster its technical support capacity to state and locals requesting assistance.

Citations:
Further Reading & Resources

This compilation of best practices draws upon and acknowledges the contributions of multiple best practices and policy-development sources.



Belfer Center for Science and International Affairs, Harvard Kennedy School, Defending Digital Democracy, *The State & Local Election Cybersecurity Playbook*, February 2018

Brennan Center for Justice at New York University, *America's Voting Machines at Risk*, 2015

Center for American Progress, *Nine Solutions to Secure America's Elections*, August 16, 2017

Center for Internet Security (CIS), *A Handbook for Elections Infrastructure Security*, Version 1.0, February 2018

Congressional Task Force on Election Security, *Preliminary Findings and Recommendations*, 2017

DEFCON, *Voting Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, September 2017

Halderman, J. Alex, University of Michigan, Expert testimony to the U.S. Senate Select Committee on Intelligence, June 21, 2017

ICA: Intelligence Community Assessment, *Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution,* January 2017

Praetz, Noah, Office of Cook County, IL Clerk David Orr, *2020 Vision: Election Security in the Age of Committed Foreign Threats*, December 7, 2017

Verified Voting Foundation, *Principles for New Voting Systems*, February 2015

Wharton School, University of Pennsylvania, *The Business of Voting: Market Structure and Innovation in the Election Technology Industry,* 2016

MEDIA CONTACT
Jaclyn Houser, Cambridge Global Advisors
jhouser@cambridgeglobal.com

EXHIBIT C

DEF CON 27 VOTING MACHINE HACKING VILLAGE

AUGUST 2019

REPORT CO-AUTHORED BY:

MATT BLAZE, GEORGETOWN UNIVERSITY
HARRI HURSTI, NORDIC INNOVATION LABS
MARGARET MACALPINE, NORDIC INNOVATION LABS
MARY HANLEY, UNIVERSITY OF CHICAGO
JEFF MOSS, DEF CON
RACHEL WEHR, GEORGETOWN UNIVERSITY
KENDALL SPENCER, GEORGETOWN UNIVERSITY
CHRISTOPHER FERRIS, GEORGETOWN UNIVERSITY

Table of Contents

INTRODUCTION

The Voting Machine Hacking Village (Voting Village) returned to DEF CON in August 2019 with a dramatic expansion in election equipment research and evaluation. DEF CON, the world's largest and best-known hacker conference, brings together a wide range of attendees including hackers; cybersecurity professionals; journalists; academics; lawyers; and local, state and federal government leaders. The Voting Village, now in its third year, saw a dramatic increase in attendance and participation, particularly from state, local, and federal government officials.

Since its launch in 2017, the Voting Village has served as an open forum to identify vulnerabilities within the U.S. election infrastructure and to consider solutions to mitigate these vulnerabilities. This year, the Voting Village demonstrated the role that hackers and other cybersecurity experts can, and should, have in the national endeavor to improve election security.

Over the course of two and a half days, hackers, technologists, academics, and other experts had full access to over 100 Voting-Village-owned voting machines to study, as well as the opportunity to attend talks and panels on topics ranging from the challenges involved in reporting on election security to the types of risk-limiting audits.

The clear conclusion of the Voting Village in 2019 is that independent security experts and hackers are stepping into the breach - providing expertise, answers, and solutions to election administrators, policymakers, and ordinary citizens where few others can.

While the discovery and replication of voting system security vulnerabilities are critical tasks for which the Voting Village plays an important role, that is not, in our view, its main contribution. Hundreds of security experts passed through the doors over the course of the weekend, many of whom had no previous experience with the particular problems and risks inherent to election technology. It is vital that we expand the pool of security experts equipped with the specialized knowledge required to evaluate, and ultimately improve, voting system security. We are especially proud of the success of the Voting Village in this essential education and outreach role.

From the outset, the mission of the Voting Village has been to highlight vulnerabilities in election equipment used in the United States and throughout the world and to serve as a resource for those whose goal is to improve the state of election security. As Voting Village organizer Harri Hursti emphasized, "As always we welcome everyone, but especially we welcome officials. We are here to help and get everyone informed - and let everyone experiment to verify the facts."

EXECUTIVE SUMMARY

1. Commercially-Available Voting System Hardware Used in the U.S. Remains Vulnerable to Attack

As in previous years, the 2019 Voting Village presented a range of currently marketed touch-screen direct recording electronic (DRE), optical scan paper voting devices, paper ballot marking devices (BMDs) and electronic poll books (e-poll books). While the Village did not attempt to (and could not) provide samples of every piece of voting equipment currently in use throughout the United States, every piece of equipment at the Village is currently certified for use in at least one U.S. jurisdiction.

And once again, Voting Village participants were able to find new ways, or replicate previously published methods, of compromising every one of the devices in the room in ways that could alter stored vote tallies, change ballots displayed to voters, or alter the internal software that controls the machines. In many cases, the DEF CON participants tested equipment they had no prior knowledge of or experience with, and worked with any tools they could find - in a challenging setting with far fewer resources (and far less time) than a professional lab (or even the most casual attacker) would typically have. In most cases, vulnerabilities could be exploited under election conditions surreptitiously by means of exposed external interfaces accessible to voters or precinct poll workers (or to any other individual with brief physical access to the machines). In particular, many vectors for so called “Advanced Persistent Threat (APT)” attacks continue to be found or replicated. This means that an attack that could compromise an entire jurisdiction could be injected in any of multiple places during the lifetime of the system.

As disturbing as this outcome is, we note that it is at this point an unsurprising result. It is well known that current voting systems, like any hardware and software running on conventional general-purpose platforms can be compromised in practice. However, it is notable - and especially disappointing - that many of the specific vulnerabilities reported over a decade earlier (in the California and Ohio studies, for example), are still present in these systems today.*

* See California Top-to-Bottom Review (2007): “Top-to-Bottom Review.” California Secretary of State. Accessed September 26, 2019. https://www.sos.ca.gov/elections/ovsta/frequently-requested-information/top-bottom-review/. and
Ohio EVEREST (2007): McDaniel, Patrick, Matt Blaze, Giovanni Vigna, Joseph Lorenzo Hall, Laura Quilter, Kevin Butler, William Enck, et al. “EVEREST: Evaluation and Validation of Election- Related Equipment, Standards, and Testing.” Secretary of State of Ohio, December 7, 2007. https://www.eac.gov/assets/1/28/EVEREST.pdf.

2. There is an Urgent Need for Paper Ballots and Risk-Limiting Audits

It is beyond the current and foreseeable state of the art to construct computerized (software and hardware based) voting devices that effectively resist known, practical forms of malicious tampering. However, this need not mean that elections must forever be vulnerable to compromise. Certain classes of voting equipment, including some (but not all) of the devices displayed at the Voting Village, can still be used to conduct high-integrity elections— in spite of their vulnerabilities — by conducting statistically rigorous post-election audits. Whether this is possible depends on the specific category of voting technology in use and, critically, whether a properly designed post-election audit process is routinely performed as a part of every election.

Systems that use paper ballots, such as optical scan voting devices, are physically designed to preserve a voter-marked record of each voter's intended choices (the original paper ballots themselves) which cannot be altered by even the most maliciously compromised software. These paper ballots are a prerequisite for the use of routine post-election Risk Limiting Audits (RLAs), which are a state-of-the-art, statistically rigorous technique for comparing (by human eye) a sample of ballots with how they were recorded by machine. This allows us to reliably determine the correct outcome of even an election conducted with compromised machines.

In particular, we emphasize that these audits can only be performed on paper-ballot-based systems. DRE ("touchscreen") voting devices cannot be used to conduct reliable or auditable elections in this way, because the stored vote tallies (as well as the ballot display) are under the control of precinct voting machine software that can be maliciously altered (in both theory and practice). The experience of the Voting Village strongly reinforces the widely understood risk that these machines might be compromised under election conditions in practice. The authors strongly endorse the recommendations of the National Academies 2018 consensus report, Securing the Vote,** that DRE voting machines, which do not have the capacity for independent auditing, be phased out as quickly as possible. This is an increasingly urgent matter, especially as foreign state actors (which may be highly motivated to disrupt our elections and which enjoy especially rich resources) are recognized as part of the threat to U.S. election integrity.

Unfortunately, the recommended practice of auditable paper ballots coupled with routine post-election risk limiting audits remains the exception, rather than the rule, in U.S. elections. While a growing number of states are already implementing paper ballots, legislation requiring routine risk-limiting audits has so far been advanced in only a few states.*** We strongly urge all states to adopt legislation mandating routine post-election risk-limiting audits. This is especially important because current optical scan paper ballot scanners (including those at the Voting Village) are known to be vulnerable in practice to compromise. Post-election audits are the only known way to secure elections conducted with imperfect hardware and software (as all modern computer-based hardware ultimately is).

** National Academies of Sciences, Engineering, and Medicine, Securing the Vote: Protecting American Democracy (Washington, DC: The National Academies Press, 2018). https://doi.org/10.17226/25120.
*** "Post-Election Audits." National Conference of State Legislatures, August 5, 2019. http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx.

3. New Ballot Marking Device (BMD) Products are Vulnerable

One of the most vigorously debated voting technology issues in 2019 is the appropriate role of paper ballot marking devices (BMDs) and how they relate to widely recognized requirements for software independence and compatibility with meaningful risk-limiting audits. Originally, BMDs were conceived of narrowly, specifically for use by voters with disabilities to assist them in marking optical scan paper ballots, bringing such systems into compliance with Help America Vote Act (HAVA) requirements for accessible voting. However, certain recent voting products greatly expand the use of BMD technology, integrating a BMD into the voting process for all voters, whether they require assistive technology or not.

As a relatively new technology, ballot marking devices have not been widely studied by independent researchers and have been largely absent from practical election security research studies. In the Voting Village this year, we had two ballot marking devices, representing two commercial models of this technology: a traditional ballot-marking device and a hybrid device. The findings only underscore the need for more comprehensive studies.

Participants in the Voting Village found that both BMD models were vulnerable to practical attack. In particular:

1. The hybrid machine outwardly appears to be a separate ballot-marking device and ballot optical scanner as two units physically integrated but architecturally separate. However, it was found that the ballot-marking device was connected to the ballot-scanning device over an internal network, and in fact was an active device in vote processing. This means that hacking the ballot marking device enables altering votes at the scanning stage.
2. Both devices stored information that could allow an attacker to compromise the secrecy of individual ballots.

The weaknesses in the current generation of ballot marking devices raises broad questions about their security and impact on overall election integrity if they were to be put into general use in elections. Aside from their potential to be maliciously configured to subtly mis-record voter choices, current ballot marking devices also offer potential avenues for election disruption via denial-of-service attacks. Voting Village participants observed that clearing many simple error situations (including those that could be deliberately induced by an attacker) required rebooting the device. This can easily create long lines at a polling place, since, as we also observed, it can take up to 15-20 minutes for these devices to complete a reboot cycle.

4. Infrastructure and Supply Chain Issues Continue to Pose Significant Security Risks

The Voting Village explored threats to election security from the supply chain. Participants continued to observe a wide array of hardware component parts of foreign origin, as well as other aspects of the supply chains for software and operational software maintenance. For example, participants found in one machine a hard-wired IP address pointing to an overseas address block.

The exact purpose and nature of whatever underlying feature used this address remains undetermined, but it underscores questions about foreign control over voting system supply chains, which should be understood to include not just the sourcing of physical hardware, but also of software and cloud-based and other remote services.

There are also significant practical issues of local election administration and resources. Local election offices are, overwhelmingly, under-resourced and under-funded, especially relative to the threats they face. Many county and local voting jurisdictions have no full-time IT staff, and many rely on outside contractors for election system configuration and maintenance. This reliance on outsourcing means that election officials often lack internal tools and other capabilities to effectively manage, understand and control their election infrastructure and as a consequence are without direct control over the security of their IT environment. With rapid deployment of new IT technology into the election infrastructure, election offices are especially exposed to remote attack (including by hostile state actors). Unfortunately, very few election offices have the resources to effectively counter this increasingly serious type of threat.

It is important to recognize that IT and cybersecurity are distinct disciplines with only a partial overlap in expertise. To promote discussion and collaboration between election officials and security specialists, the Voting Village conducted the first “Unhack the Ballot” initiative to create an opportunity for election officials to connect with, ask questions, and find answers from security specialists. This “off the record session” was held for the first time in a private room at the Voting Village.

EQUIPMENT AVAILABLE AT THE VOTING VILLAGE

Direct-Recording Electronic Voting Machines

A direct-recording electronic (DRE) voting machine allows voters to electronically cast their ballots by manually touching their choice of candidate on a screen, monitor, or other similar device. The DRE records and tallies the votes directly into its computer memory, without a paper ballot. Only some DRE models feature a Voter-Verified Paper Audit Trail (VVPAT).

Dominion: Premier/Diebold AccuVote TSx

The AccuVote TSx is a DRE voting machine manufactured by Premier Voting Solutions, later acquired by Dominion Voting Systems. The product line currently belongs to ES&S.

As of 2018, the AccuVote TSx was in use in 18 states.*

Dominion: AVC Edge

The AVC Edge is an electronic voting machine manufactured by Sequoia Voting Systems, later acquired by Dominion Voting Systems. It is a touch-screen machine with direct-recording electronic capabilities. It is activated by a smart card, and records votes on internal flash memory. Each unit contains a slot for a vote activation card. After the voter's ballot is cast, the smart card is deactivated to prevent multiple votes from being cast. Votes are subsequently documented. When polls close, the votes recorded in each machine are either physically or electronically transmitted to election headquarters.

As of 2018, the AVC Edge was in use in 10 states.**

ES&S: iVotronic DRE

The iVotronic DRE is an electronic voting system that allows voters to make their choices on a touch screen interface and records and tabulates votes in internal memory.

As of 2018, the iVotronic DRE was in use in 16 states.***

* "Polling Place Equipment - November 2018." The Verifier. Verified Voting. Accessed September 26, 2019. https://www.verifiedvoting.org/verifier/#year/2018/.

** According to survey of publicly available information conducted by DEF CON Voting Village.

*** "Polling Place Equipment." The Verifier. Verified Voting. Accessed September 26, 2019. https://www.verifiedvoting.org/verifier/.

Electronic Poll Books

An electronic poll book, also commonly called an e-poll book, is typically either a dedicated device with embedded software or a standard commercial laptop/tablet with a software application that allows election officials to review, maintain, and/or enter voter register information for an election, functions that had traditionally been handled using a paper-based system. These systems are limited to the check-in process and do not participate in counting the votes. The usual functions of an e-poll book include voter lookup, verification, identification, precinct assignment, ballot assignment, voter history update and other registry maintaining functions such as name change, address change and/or redirecting voters to correct voting location. In the states that allow same-day registration, e-poll books are also used to enter new voter information and interact with statewide voter registration systems.

ES&S: Diebold ExpressPoll-5000

The Diebold ExpressPoll-5000 is an e-poll book, designed for use by individual poll workers. It is used in precincts to check voters in before they are permitted to vote. The product line currently belongs to ES&S, but the ones used at DEF CON were models running Diebold/Premier-branded software, which is also still in use in several places in the U.S. Its operating system is a version of Windows CE, a system built by Microsoft for embedded applications.

ES&S: ExpressPoll Pollbook Tablet with Integrated Pollbook Stand

ExpressPoll Pollbook Tablet is an e-poll book designed for use by individual poll workers and is used in precincts to check voters in before they are permitted to vote. This product was introduced to the market in 2015 and consists of a Toshiba Encore 2 standard 10-inch tablet running Windows 8.1 operating system. It is mounted to an integrated stand which has an internal USB hub for connected peripheral devices like a printer, smart card reader, ethernet, extra battery and magnetic stripe reader.

Ballot Marking Devices

Ballot marking devices (BMDs) are machines that allow voters to make choices on a screen and then print out a paper ballot with the voter's choices, which is the ballot of record. The paper ballot is then hand counted or tabulated using an optical scanner (see description below). In general, BMDs should neither store nor tabulate votes, but only allow the voter to record votes on ballots that are then stored and tabulated elsewhere. Some BMDs produce paper print-outs of barcodes or QR codes instead of a voter-verifiable paper ballot, which has become a source of much controversy.

The first ballot marking devices emerged in the late 19th century, but were only widely used in the last few decades. Today, electronic BMDs have come into widespread use as assistive devices in the context of optical scan voting systems to provide compliance with HAVA, though in recent years vendors have proposed that the devices be used by all voters.

ES&S AutoMARK

The AutoMARK is an optical scan ballot marker that is designed for use by voters who are unable to personally mark an optical scan ballot. The AutoMARK works in conjunction with an optical scanner. It was developed by Vogue Election Systems and the product line was purchased by ES&S. The machine features several features to enhance accessibility for voters with physical impairments or language barriers.

As of 2018, the AutoMARK was in use in 28 states.^

Optical Scanners

Optical scanners are digital scanning devices that tabulate paper ballots that have been marked by the voter. Ballots are either scanned at the precinct (in a precinct count system) or at a central location (in a central count system).

Diebold AccuVote OS

The AccuVote OS is an optical scan voting system. It can be used by precinct count systems and central count systems. Voters cast their ballots by inserting them into the AccuVote OS system, where votes are digitally tabulated, recorded, and stored. Originally marketed as the Unisys ES-2000, the machine later became known as the Global Election Systems AccuVote-OS Precinct Count (AVOS-PC) paper ballot scanner. In recent years, the machine has also been marketed and/or supported under the brands Diebold, Premier, ES&S, and Dominion.

As of 2018, the AccuVote OS was in use in 26 states.^

ES&S: M650

The M650 is an electronic ballot scanner and tabulator manufactured by ES&S. The ES&S M650 is used for counting both regular and absentee ballots. It launches ballots through an optical scanner to tally them, and keeps count on an internal 128 MB SanDisk Flash Storage card (pictured below). Election staff are responsible for configuring the M650 for each election.

As of 2018, the M650 was in use in 23 states.^

Hybrid Systems

Dominion: ImageCast Precinct

The Dominion ImageCast Precinct is an optical scanner paper integrated with DRE ballot marking device. It scans human-marked ballots, allows voters with disabilities and other voters requiring assistance to use the ballot-marking device to mark and review their ballots, and stores ballots for tabulation after the election period.

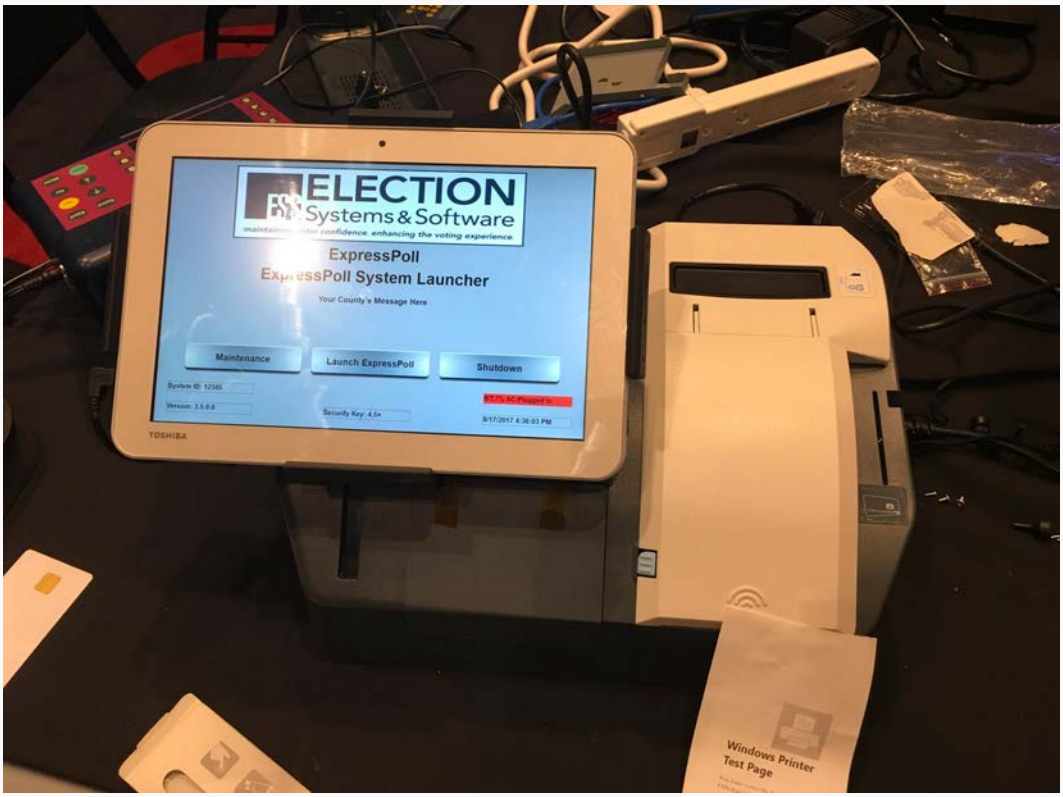
As of 2018, the ImageCast Precinct was in use in 10 states.^^

^ "Polling Place Equipment." The Verifier. Verified Voting. Accessed September 26, 2019. https://www.verifiedvoting.org/verifier/.

^^ According to survey of publicly available information conducted by DEF CON Voting Village.

OVERVIEW OF TECHNICAL ISSUES FOUND OR REPLICATED BY PARTICIPANTS

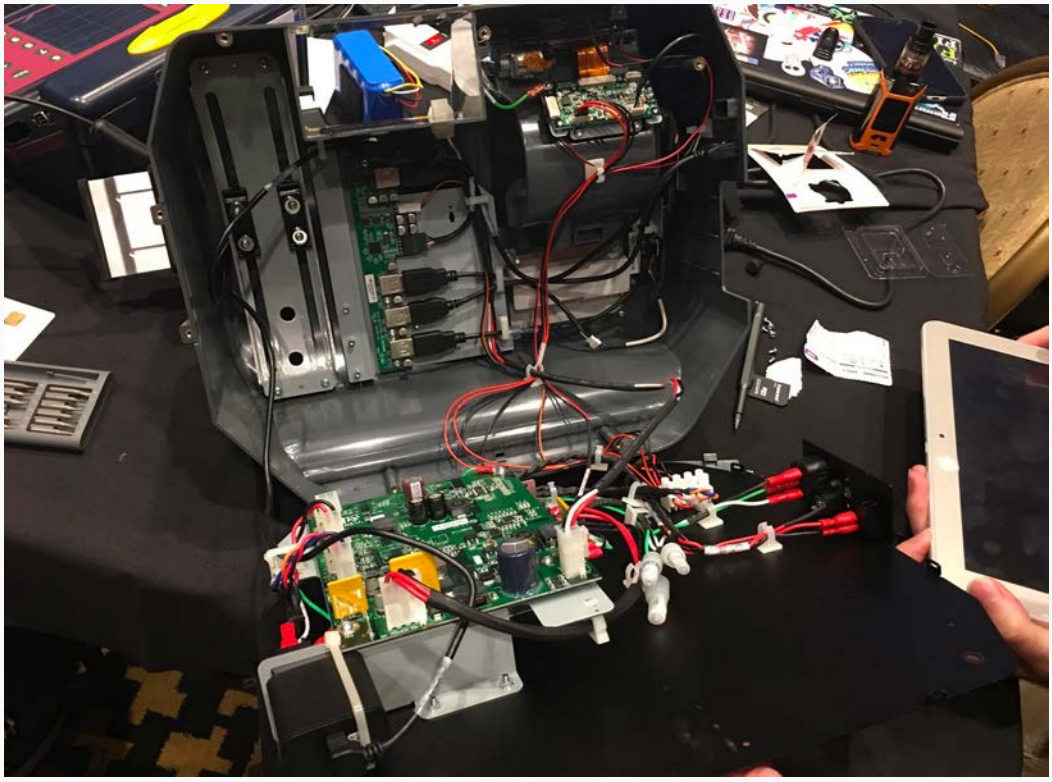
ES&S: ExpressPoll Tablet Electronic Pollbook



Picture: ES&S Electronic Pollbook System on an integrated stand with built-in printer, smart card reader, and other integrated peripheral devices.

The ES&S ExpressPoll Tablet Electronic Pollbook is an e-poll book which uses a standard commercial unencrypted Toshiba tablet held in place to a dock by a rubber locking mechanism. The specific model of the tablet was a Toshiba Encore 2 with Intel Atom CPU and running Windows 8.1 32-bit operating system.

The tablet can be popped out of its dock, exposing an SD port and a USB port of the tablet itself. Additionally, a USB hub is built into the mounting stand, which exposes additional USB ports. All these ports are active. The ports outside the mount are accessible to voters and poll workers without any physical locks or mechanical support for tamper-evident seals.



Picture: Internal electronics of the e-poll book stand. Internal USB hub visible is also directly connected to externally exposed USB connector. The researchers in the Village were able to print out with the voter permission slip directly by connecting into external USB.

While the SD card, which contains voter data, is encrypted, all keys are stored in plain text in a standard xml file allowing all data to be easily accessed and modified, thereby rendering encryption meaningless.

A card or USB device may be placed into the machine directly even when the dock is locked; the locking mechanism does not prevent access to the externally exposed ports on either on the tablet or on the stand.

None of the BIOS passwords were set. This allows unrestricted access to all system settings. By default, the device booted from a USB first without any password required.

The supervisor maintenance password is stored in plaintext on this device. In this case, the password for the tablet was “ESS”.

Security features supported by the underlying commercial hardware were turned off or not activated. The tablet supported Secureboot, a common security feature designed to check to see if the system has been tampered with and prevent the machine from running code of unknown origin. This was disabled by default on the tablet, allowing the e-poll book to load unsigned code from any source.

Picture: Externally exposed USB port on the side of the Electronic Pollbook Stand. The port does not get locked when the stand is locked and it does not have a lid or hook on which to place a seal.

As the Toshiba tablet is a standard off-the-shelf 'PC compatible' general-purpose device, it is supported by a wide range of general-purpose operating systems. This machine can be booted from a version of Linux using, for example, the external USB port and USB memory stick. Booting from Linux allows an attacker to access data on the device without encountering any Windows operating system-based defenses. Voting Village participants confirmed that an attacker would then be able to freely access data and run custom software, including software that would allow extraction of voter data. An attacker could also change or delete any voter registration data (like party registration) stored on the machine once the machine has been accessed.

The e-poll book operating system stack lacked any attempt to perform even the most rudimentary platform hardening. In fact, none of the bloatware that would come with a standard Toshiba tablet was removed. Apps for Netflix, Hulu, and Amazont were present in the e-poll book.

The lack of hardening is especially dangerous given that for one of the recommended deployments the system is intended to communicate over WiFi with wireless internet access to either Amazon Web Services or Microsoft Azure-based cloud services. Given that the operating system is unhardened and given that the standard bloatware provided by the vendor is present on the machine, there is an extremely wide, unprotectable, exposed attack surface.

ES&S AutoMARK

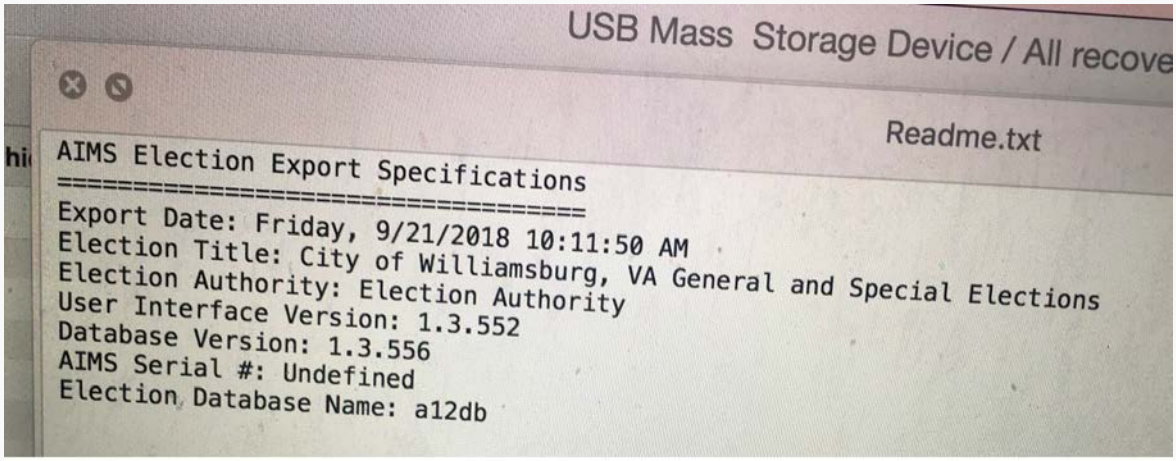
Picture: ES&S AutoMARK Ballot-Marking Device

The ES&S Automark is a ballot marking device that allows keyboard and ethernet ports to be plugged in after removing the top of the machine's case. The casing is closed only by 3 screws and does not include any tamper-evident seals. Immediate root access to the device was available simply by hitting the Windows key on the keyboard.

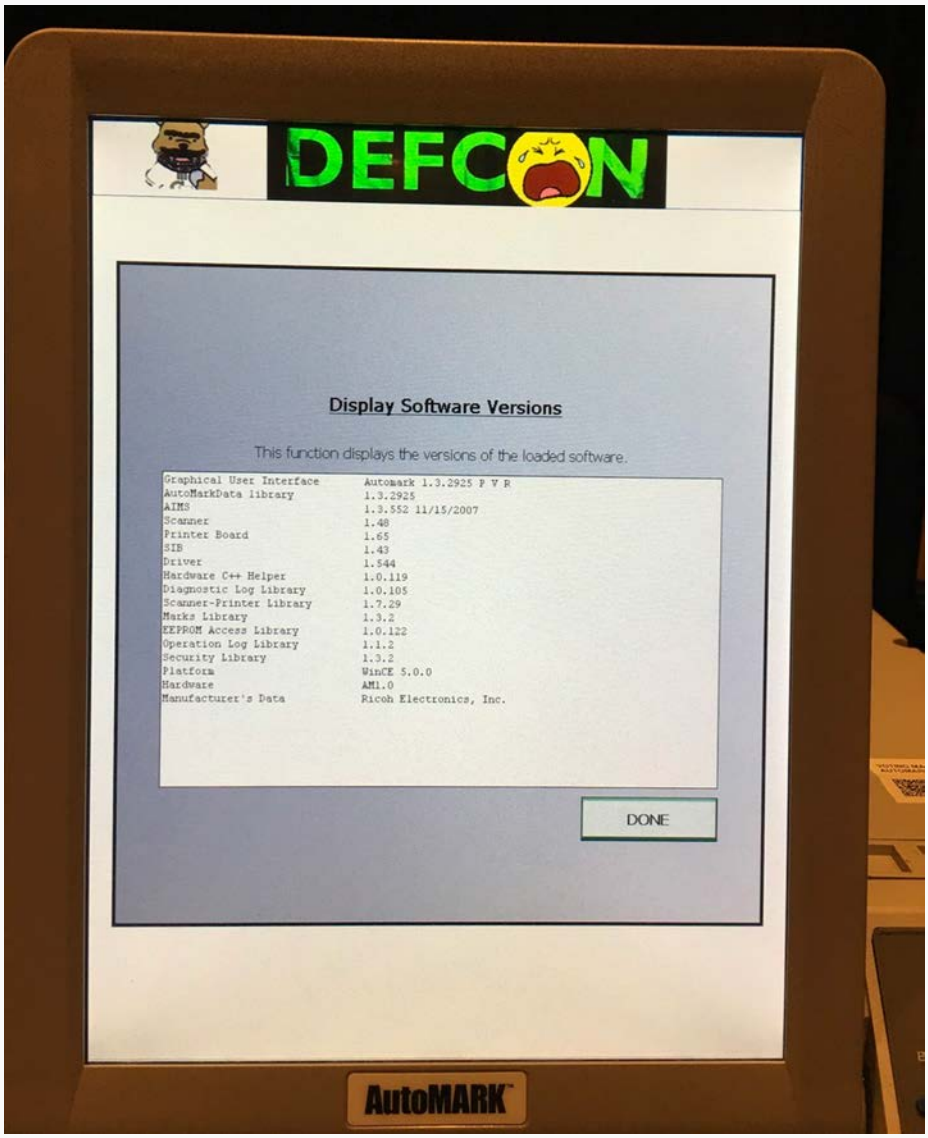
The lock to this device can be picked manually, allowing root and physical access to the unencrypted drive.

A RJ45 jack appears to be hidden behind a sticker on the front of the machine, accessible by removing the sticker without any tools.

The ES&S AutoMARK runs Windows CE Embedded Operating System 5.0. The application software in the machine appears to be last updated around the end of 2007, and the system appears to have been last used in a special election in late 2018.



Picture: Election database manifest file from the AutoMARK showing details of the last election for which it was used.



Picture: AutoMARK software version screen.

Operating system implementation has not been hardened or unneeded elements removed to minimize attacking surface. For example, Internet Explorer is present on this device.

Because the operating system is not hardened, an attacker can, before the machine boots up, drop malware onto the device after holding the “screen” button for five seconds.

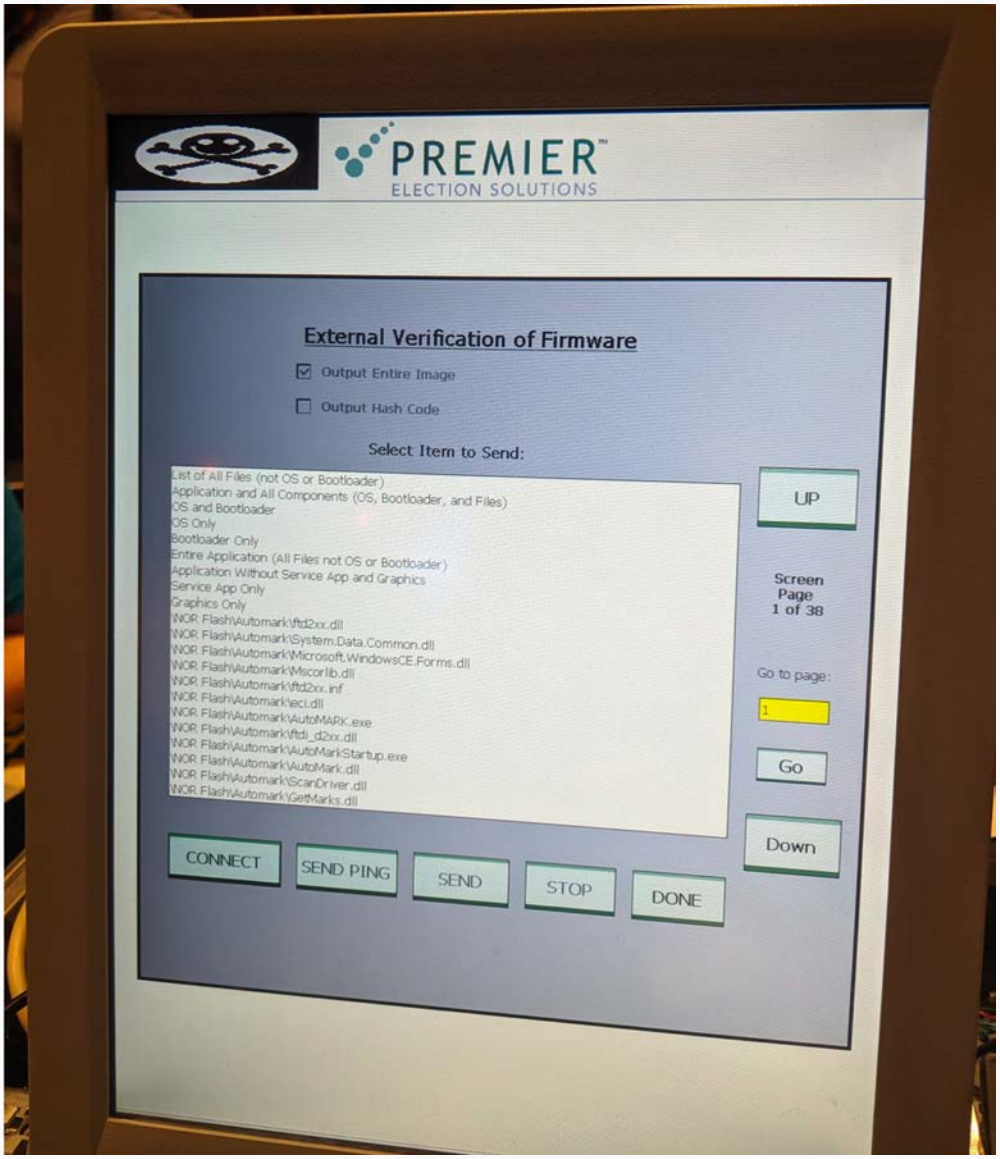
Collectively, a few people were able to change the group IDs of political parties still stored in the device from the previous election. However, this triggered a warning screen, indicating some form of integrity-checking for the stored data.

The embedded Windows operating system has special feature "Allow data connections on device when connected to PC" to enable Windows Mobile Device Center to allow the general purpose Windows version communicate with embedded windows. This feature was turned on.

The machine used several passwords/pins which were very simple, including passwords listed as default passwords in online manuals. These codes include “1111” as the pin code to replace the entire firmware of the device.

Participants were able to adjust the load address which caused the voting applications software to consistently crash. In this instance, the reason for the machine crashing would not be obvious to nontechnical people, such as the volunteers helping to run the polls, thereby creating an effective denial of service attack which would be hard to remotely diagnose.

Additionally, the administrator password was stored in the clear in the configuration file and participants were able to use it to enter admin mode. This enabled them to look at the binaries and replace the header on the voting machine with one of their choosing. Nick Bishop was one of the participants responsible for these discoveries, and has willingly identified himself.



Picture: AutoMARK firmware function enabling automated extraction of the whole system image.

Participants managed to place the DEF CON logo in the header portion of the screen and were able to edit the registry. Using a screwdriver to open up the machine, participants were able to plug a keyboard into an exposed USB port and operate the voting machine as a standard Windows CE machine after exiting the specialized voting software.

Participants Minoo Hamilton and William Baggett also discovered the default system maintenance password by searching on Google, revealing “admin” as the identification name and “vogue” as the password. This allowed both of them to gain access to the securities section on the machine, enabling them to make changes and access vital information. From the securities section they were able to run a remote integrity check that displayed the files and the integrity of each file. Mr. Baggett discussed potential implications for these risks for issues involving a forensic change of evidence. Depending on the protocol adopted by an election office, it is possible that if an attacker modified the access database or central tabulator after hacking their way in, the integrity of the modified data would not be checked against the centralized system.

Dominion Imagecast Precinct

Picture: Dominion ImageCast Precinct with Ballot-Marking Device screen turned to face the scanner (back) side of the machine.

The Dominion ImageCast Precinct is an integrated hybrid voting equipment. It combines an optical paper ballot scanner and ballot marking device and allows for nonvisual accessibility for the blind and visually impaired, in compliance with HAVA. This machine provides voters with disabilities the same opportunities for access and participation as other voters.

This device integrates the devices and the ballot box to store the cast ballots into one unit, but has a single locking mechanism that holds the entire ballot box together. If picked, ballots could easily be stolen using common items such as a standard trash picker.

Participants were able to access USB, RJ45, and CF slots on this machine without using destructive force.

The system also runs Busybox Linux 1.7.4, which has twenty currently known medium to high level vulnerabilities including the ability to allow remote attackers to allow a DNS through CPU/bandwidth consumption via a forged NTP packet which triggers a communication loop with the effect of Denial-of-Service attacks.*

* Search Results. Common Vulnerabilities and Exposures. Accessed September 26, 2019. https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=busybox.

Boot settings also allow for the system to be booted from an external USB on startup.

Importantly, the CF card and card readers on the front and back of the machine are physically exposed, and could be replaced.

Additionally there is an internal USB port that is not exposed and an external CF slot that is covered by a tiny door. Either slot can be used to load the OS. Boot order is USB then CF.

The door opens by unscrewing one of the screws. The screws in question were so-called secure screws. Participants made a quick run to a nearby electronics store to purchase “Security Bits Set with Ratchet Driver” for under $28 which was used to open all ‘security screws’ used in any of the machines.

Picture: Small unmarked lid on the side of the machine for accessing CF card slot inside of the machine. So-called “secure screw” tips can be commonly purchased from any electronic store.

When participants removed the CF card on the front of the machine, they found scanned ballots and the configuration file in the clear. In the absence of other protections, modifying configuration data could allow an attacker to edit which X/Y locations on the scanned ballots matched with which candidate. Participants found no digital signing or encryption protecting those digital files.

Participants responsible for much of the work on this machine identified themselves willingly: Zander Work, Lyell Read, Cody Holiday, Andrew Quach, Steven Crane, Henry Meng, and Nakul Bajaj. As a group, they were able to boot an operating system of their choice and play video games on the voting machine, including a popular game called “Pong”. These participants averred that by bringing a simple screwdriver and CF card into the voting area, an attacker could use a screwdriver to access the machine’s intended CF card and swap it with the card they brought, allowing the attacker to boot an arbitrary operating system and take control over the machine.

The group was able to browse the file system on the CF card, proving that the filesystem was unencrypted and unprotected.

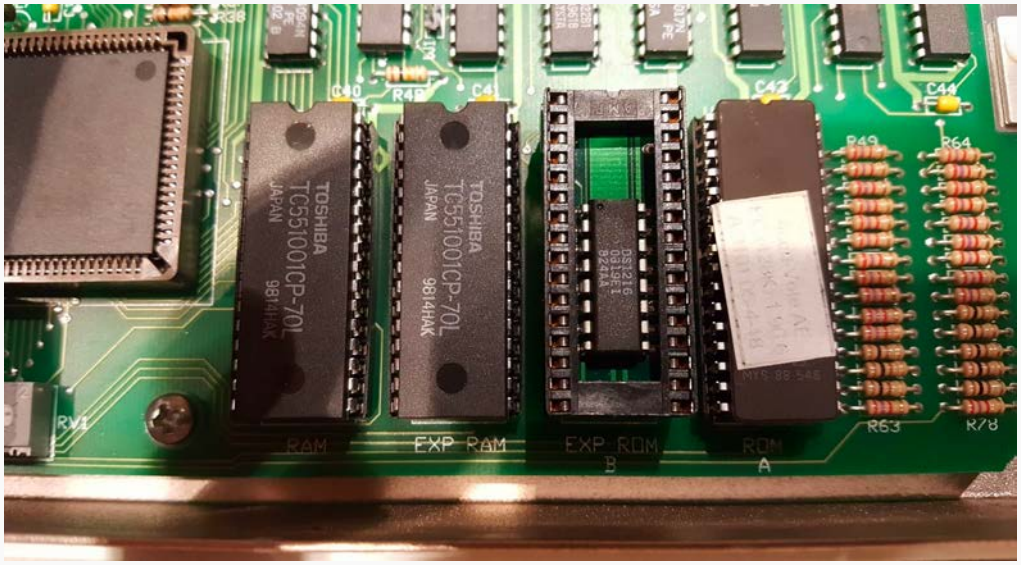
AccuVote-OS Precinct Count

Picture: Originally marketed as Unisys ES-2000 later become Global Election Systems AccuVote-OS Precinct Count (AVOS-PC) paper ballot scanner. Later also marketed/supported under brands Diebold, Premier, ES&S and Dominion.

Participants also discovered a set of previously undocumented functions in the Dominion/Diebold/Premier/ES&S AccuVote, enabling remote manipulation of the machine's memory card when the machine is connected to a network — without any physical access to the memory card, and without breaking or circumventing any physical seals. Researchers confirmed the existence of these features with a person who has previously been involved with the maintenance of these machines, and an election official who had encountered the feature before. The investigation of these functions and possible mitigations is ongoing at the time of this report.

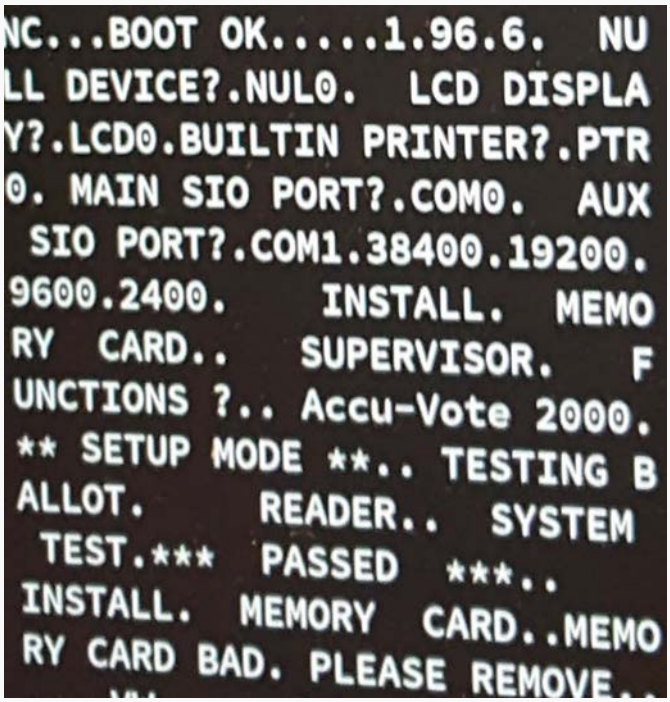
The Voting Village acquired two dozen devices from the same jurisdiction. From the circumstantial evidence of documents in the travel cases, it appears that the machines were put in use and subsequently retired together. However, the devices did not have the same software version installed. Despite possibly having been used in the same elections, some of the machines had software version 1.96.6, whereas others were running 1.96.4, an older version.

In this device, the software is installed on a socketed EPROM microchip. EPROM stands for Erasable Programmable Read-Only Memory and it is a type of programmable read-only memory (programmable ROM) that can be erased and reused. This type of chip has to be physically removed from the circuit board, placed into a separate programmer device, and completely erased before it can be reprogrammed. Erasing the chip is done by shining an intense ultraviolet light through a window through which the silicon chip is visible. The erasing window must be kept covered with an opaque label to prevent accidental partial or unstable erasure by the UV by sunlight or camera flashes and therefore the window is always covered by a sticker as seen in the picture.



Picture: AVOS circuit board with socketed EPROM chip containing election software. Software upgrades to this machine are installed by physically replacing the chip; as the chip is socketed, this can be done in a matter of seconds. The chip inside a socket is a SmartWatch CMOS real time clock with an NVRAM controller circuit and an embedded lithium energy source.

This machine was originally developed in 1986 and first introduced to market in 1989, and it is believed to have been used for the first time in U.S. general elections in Minnesota in 1990. The CPU of the system is NEC V25, which was the microcontroller version of the NEC V20 processor. The V20 was a processor made by NEC that was a reverse-engineered, pin-compatible version of the Intel 8088 with an instruction set compatible with the Intel 80186. It has 16-bit internal architecture and 8-bit external data bus. The V20 was introduced in 1982 and V25 was officially phased out in early 2003. The EPROM containing the programming was 128KBytes in size and the system had two RAM chips 128KBytes each.



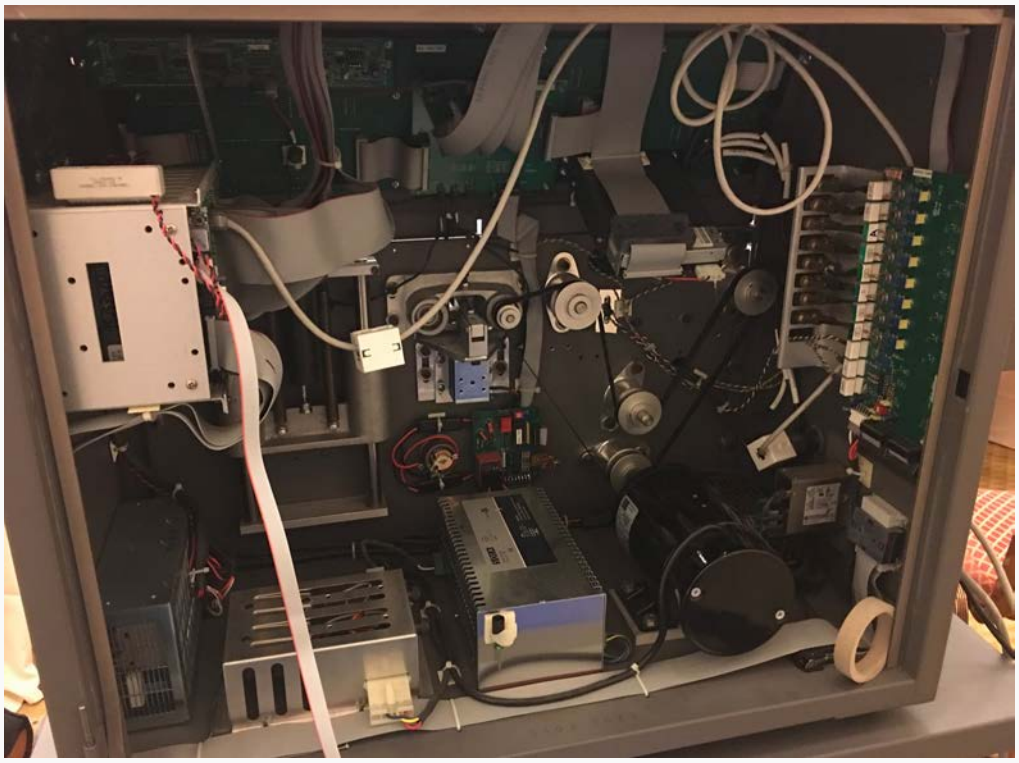
Picture: Human readable strings from the chip contained in the programming. As is typical for embedded systems of the era, the programming contains a lot of clear text strings. In this era of technology, compression and encryption were things of the future.

EVID

Picture: VR System EViD electronic poll book system.

Participants confirmed that the hardware for this machine is a normal general purpose PC hardware which is very low-end by today's standards. There was no BIOS password set on the machine. Consequently, participants were able to boot an arbitrary operating system off a live CD, which had the ability to run on 32-bit and limited to 128M RAM. Ultimately, the device was used as an entertainment device, amusing visitors with Nyan Cat.

ES&S M650



Picture: Inside of ES&S M650 Optical Paper Ballot scanner. Storage devices and other electronics are quick and easy to replace in a card rack in the upper left. Note the overpowered for the purpose electric motor for moving the paper ballots.

Last year, the Village made accessible to participants two M650 units which had been used in Oregon. This year, the Voting VIllage acquired an additional unit used in the state of Washington. Based on documentation, all three devices were from the same year and same hardware revision. Based on that, the researchers were surprised to discover that the hardware and the features between the devices were not identical. It is unclear who had carried out the modifications.

The paper maintenance log inside the machine did not answer that question, but showed that maintenance personnel periodically have physical access to the inside of the machine. With physical access, this type of machine has no security protections against any kind of modifications.

RECOMMENDATIONS

While the DEF CON Voting Village is heavily focused on the technical aspects of the election infrastructure, the Unhack the Ballot initiative underlined the importance of all levels of the human factor aspects in an election ecosystem. Election officials need more training and better access to parties who can help them to navigate the consequences of technological choices around them. Bearing in mind that at the moment many of those choices take place in the long out-sourcing supply chains of the ecosystem and election officials are left into the tail-end of the process to design mitigation strategies into deployments which they were not participating in design. Election officials also need help to train their own staff to be more security-minded and to gain the 'muscle memory' instincts to protect day-to-day operations, both during election cycles and between them.

The security implications of ballot marking devices should be further studied. This calls for multi-disciplined research looking into the various aspects of the election process from integrity and security to usability and reliability. Current and proposed next-generation ballot marking devices have not been designed with security considerations in mind. They open the door for various methods to attack the election process. In the simplest end are denial-of-service attacks and attacks to compromise the secrecy of the ballot. Depending on the deployment strategy, the ballot-marking device will know a lot about the voter and therefore ballot-marking devices can be hacked specifically to, for example, disenfranchise vulnerable populations: voters who use audio interface, sip-and-puff, large fonts, non-English language ballots, or who take a long time to vote. The discussion about 'detecting' hacked devices is dangerous, because in the absence of remedies even if irregularities are reported there is almost no way to properly investigate. Ballot-marking devices as currently deployed have an insurmountable security design and delegation flaw: the protocols make voters responsible for checking whether devices are performing correctly, and voters cannot get any evidence to prove to others that a malfunction occurred and therefore even if voter detects and reports an error, it would often be the only remaining course of action for poll workers to assume a mistake on the voter's part.

The use of barcodes should be carefully analyzed from various security aspects. Malicious fraudulent advanced barcodes have been causing a lot of problems to Point-of-Sale systems and utilizing bar codes in elections opens a new avenue for injection and scripting type of attacks. The

election integrity, auditability and transparency aspects of using barcodes are even more important. Paper ballots have been promoted because they make those various methods of audits possible. This is true only if the significant record of the vote is human readable. At this point in time, we have to recognize that there are two aspects: technological soundness and the public trust. In elections, it is important that the losing parties and their supporters accept the results as fair. Any method of voting which is not completely transparent and understandable by everyone can be contested in the court of public opinion.

Hybrid machines, which offer users the option of inspecting their ballot before printing, should be avoided because they increase the risk of undetectable attacks. Because the machine knows which ballots are inspected and which are not, it can modify only those that are not inspected — essentially undermining the purpose of voter-verifiable ballots. Such attacks would be very hard to detect exactly because the attacked ballots are those not inspected. With today's razor-thin margins of victory in elections, even the ability to modify a small percentage of the votes undetectably can have a huge impact.

Inspection of newer models of e-poll books further underlines the absence of security design both in software, hardware and physical security aspects. E-poll books are inherently networked devices to synchronize across all devices at a polling place and to avoid cabling, which is often done wirelessly. Furthermore, many new makes and models of the e-poll books actively communicate in real-time over the Internet to back-end servers hosted in commodity cloud services. So far, the e-poll books studied in the Voting Village have been utilizing general-purpose operating systems on commercial off-the-shelf hardware with no special hardening or security measures.

Historically, security measures provided by the hardware / low-level programming have been systematically turned off in all classes of devices used as part of the election infrastructure. Unfortunately, this was found to be true also with newer generations of voting equipment in the Village. These practices greatly simplify paths to attack the machines and also place increased to unbearable burdens to physical security and chain-of-custody management of the machines over the entire lifetime of the devices.

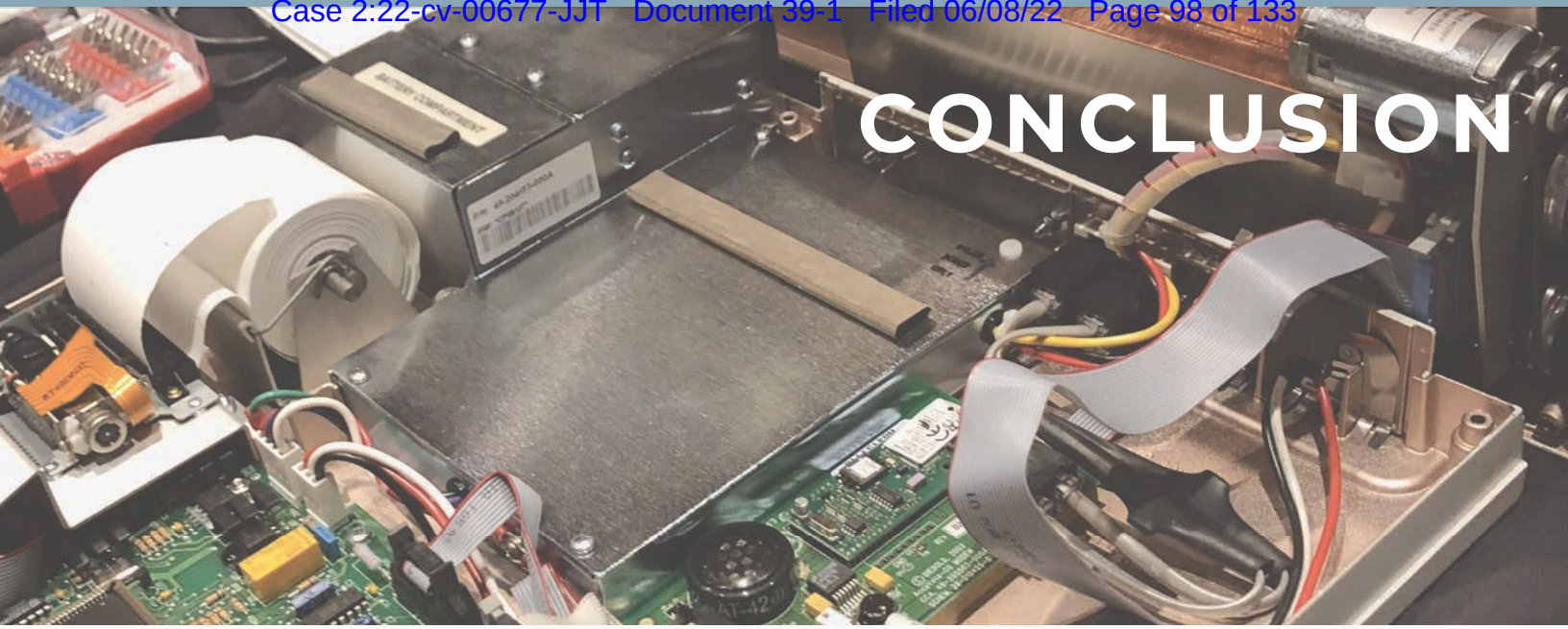
Election reporting was increasingly an area of concern in the Village discussions. With the election night beginning of the process happening over the internet as well as the end of the process as reporting happening over the Internet, discussions in the Village were drawn into similar information flow designs in other industries and how irregularities in those setting had managed to go unnoticed when the ends of the process are seemingly matching. There needs to be a process in place to verify that the reporting truly is sum-of-its-parts.

DARPA SECURE HARDWARE TECHNOLOGY DEMONSTRATOR

For the past four years, DARPA has been working to build next-generation secure hardware through its System Security Integrated Through Hardware and Firmware (SSITH) program. This new hardware was unveiled for the first time to the public in the Voting Village.

The SSITH program develops methodologies and designs tools that enable the use of hardware advances to protect systems against software exploitation of hardware vulnerabilities. To evaluate progress on the program, DARPA has incorporated the secure processors researchers are developing into a very early prototype application of a secure voting ballot box. At the Voting Village this year, they turned the system loose for public review by thousands of hackers and DEF CON community members. The purpose of this application is solely to provide a demonstration system that facilitates open challenges. To be clear, the SSITH program will not produce a voting system, nor will it provide a specific solution to election system security issues for use during elections.

During DEF CON 2019, the SSITH system demonstrator consisted of a set of RISC-V processors that the research teams will modify to include their SSITH security features. Since SSITH's research is still in the early stages, only one prototype version of the 15 processors in development was available for evaluation. DEFCON 27 was the first small step on a path to evaluate the hardware design. In 2020, DARPA plans to return to DEF CON with an entire demonstrator system, which will incorporate fixes to the issues discovered during this year's evaluation efforts.



CONCLUSION

As in previous years, this year's Voting Village demonstrated vulnerabilities inherent in the election environment and highlighted the enormity of the task of securing our nation's elections. Among the many issues highlighted at the Voting Village this year, particularly on machines previously unavailable to the hacker community, three serious vulnerabilities stood out:

1. Widespread use of current ballot-marking device architectures poses new systemic security risks
2. Previously studied commercial election equipment continues to surprise with new weaknesses
3. Many systems are shipped with basic security features disabled

If we as a nation are serious, as we must be, about improving election security in the United States, particularly ahead of the 2020 presidential election, the Voting Village recommends that the following as urgent priorities:

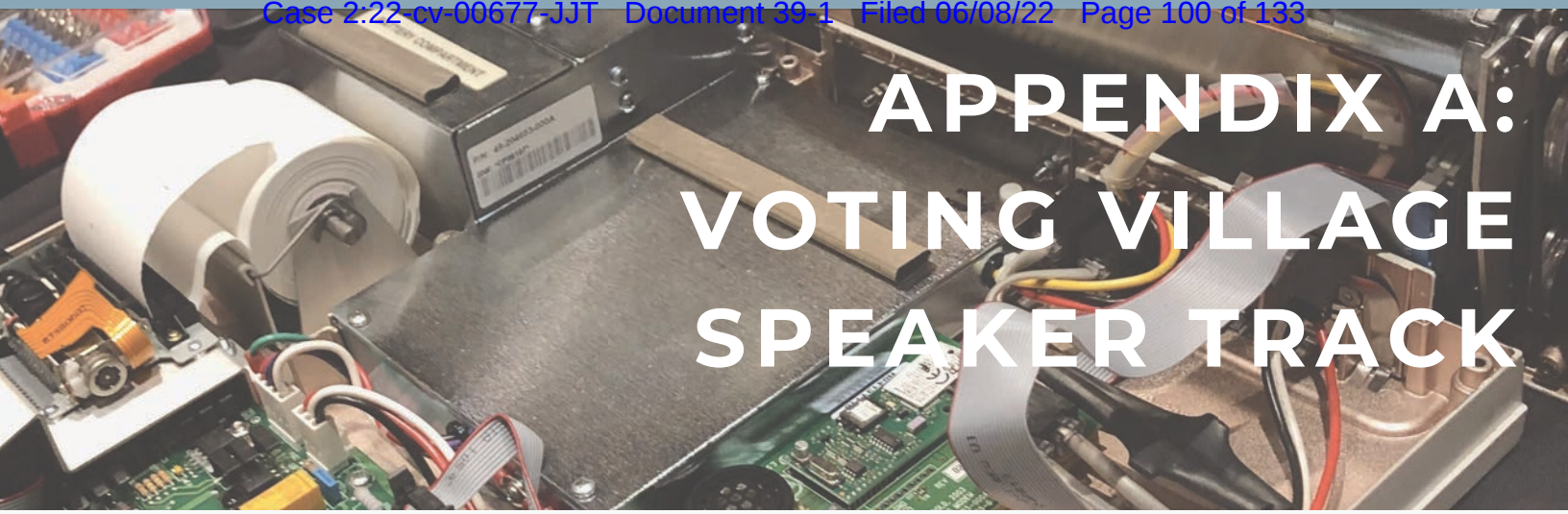
I. Nationwide deployment of mandatory post-election risk-limiting audits
II. Nationwide deployment of voter-marked paper ballot systems
III. Dramatically increased funding and other resources to help local election officials protect their IT infrastructure from foreign state actors and other threats.

Without taking these steps to support election administrators at the frontlines of this clear national security threat, we fear that the 2020 presidential elections will realize the worst fears only hinted at during the 2016 elections: insecure, attacked, and ultimately distrusted.

ACKNOWLEDGMENTS

A number of individuals contributed to the success of the DEF CON Voting VIllage and the production of this report. A special thanks to:

- The organizers, subject matter experts, and partners who collaborated to make the Voting Village concept a reality and helped to author this report;
- The speakers and moderators of the Voting Village speaker track, including Senator Wyden, Representative Eric Swalwell, representatives of the U.S. Department of Homeland Security, the Defense Advanced Research Projects Agency (DARPA), and many others;
- The state and local election administrators who attended the Voting Village to share their wealth of experience and learn from the hacker community about the latest election system security concerns;
- The outstanding support and contributions of Jake Braun, Phil Stupak, Morgan Ryan, Jaclyn Houser, Analiese Wagner, Casey Dolen, Claire Martin, and Caroline Hymel;
- The indispensable legal advice and guidance provided by Kendra Albert, Sunoo Park, and Thomas Hopkins of the Cyberlaw Clinic at the Berkman Klein Center for Internet & Society, Harvard Law School; and
- Verified Voting and the Michael and Paula Rantz Foundation, for their generous support of this work.



APPENDIX A: VOTING VILLAGE SPEAKER TRACK

This year's Voting Village speaker track spanned all three days of the conference and featured members of Congress, representatives from the Department of Homeland Security and the Department of Defense, private sector pioneers, academics, researchers, and hackers of all stripes. Below is an overview of each day's talks, as well as each speaker's biographical information.

Friday, August 9, 2019

Welcome and Voting Village Kick-off Remarks

- **Harri Hursti, *Co-Founder, DEF CON Voting Village; Founding Partner, Nordic Innovation Labs***

  Harri Hursti is among the world's leading authority in data and election voting security, critical infrastructure, and network security systems. Beginning his career as one of the minds behind the first commercial, public email and online forum system in Scandinavia, he went on to cofound EUnet-Finland. Hursti has authored many studies on election security and vulnerability in both academic and corporate publications. He worked for Black Box Voting where he performed voting machine hacking tests, which became known as the Hursti Hacks. These tests were filmed and later turned into the acclaimed HBO documentary Hacking Democracy.

- **Matt Blaze, *Co-Founder, DEF CON Voting Village; Professor of Law and McDevitt Chair for the Department of Computer Science, Georgetown University***

  Matt Blaze holds the McDevitt Chair of Computer Science and Law at Georgetown University. His research focuses on the architecture and design of secure systems based on cryptographic techniques, analysis of secure systems against practical attack models, and on the intersection of computing and communication technology and public policy. In addition to his position at Georgetown University, he sits on the board of directors of the Tor Project. Blaze received his PhD in Computer Science from Princeton University.

- **Jake Braun, *Co-Founder, DEF CON Voting Village; Executive Director, University of Chicago Harris Cyber Policy Initiative***

  Jake Braun serves as the Executive Director for the University of Chicago Harris School of Public Policy's Cyber Policy Initiative where he works at the center of politics, technology and national

security to advance the field of cyber policy. Prior to joining CPI, Braun was appointed White House Liaison to the Department of Homeland Security (DHS) by President Obama where he was instrumental in the passage of the unprecedented Passenger Name Record (PNR) Agreement, one of the largest big data agreements in history. In addition, he worked on the development and implementation of the Homeland Security Advisory Council's Task Force on CyberSkills. Braun is also a fellow at the Council on CyberSecurity and is a strategic advisor to DHS and the Pentagon on cybersecurity.

Remarks by CISA Director Chris Krebs

- **Christopher Krebs, *Director, Department of Homeland Security's Cybersecurity and Infrastructure Security Agency***

  Christopher Krebs serves as the first director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Mr. Krebs joined DHS in March 2017, first serving as Senior Counselor to the Secretary, where he advised DHS leadership on a range of cybersecurity, critical infrastructure, and national resilience issues. Prior to coming to DHS, he was a member of Microsoft's U.S. Government Affairs team as the Director for Cybersecurity Policy, where he led Microsoft's U.S. policy work on cybersecurity and technology issues.

DARPA SSITH Program at DEF CON

- **Linton Salmon, *Program Manager, Defense Advanced Research Projects Agency (DARPA)***

  Dr. Linton Salmon joined the Defense Advanced Research Projects Agency as a program manager in September 2014. Prior to joining DARPA, Dr. Salmon spent 15 years in executive roles directing development of CMOS technology at GlobalFoundries, Texas Instruments and Advanced Micro Devices. Before joining Advanced Micro Devices, Dr. Salmon was vice president for Research and Technology Transfer at Case Western Reserve University and an associate professor of electrical engineering and physics at Brigham Young University (BYU), where his research areas included CMOS processes, micro-battery research, packaging and MEMS.

What Role Can Journalists Play in Securing Elections?

- **Maggie MacAlpine *(moderator), Co-Founder, Nordic Innovation Labs***

  Margaret MacAlpine is an election auditing specialist and system testing technologist. She has worked on a variety of projects that include electronic testing of voting registration systems, election security and election fraud for a variety of countries, states and counties. Ms. MacAlpine has served as an advisor for the office of the Secretary of State of California for the Risk Limiting Audit Pilot Program 2011-2012, and is widely regarded as an expert on the use of high-speed scanners for conducting post-election audits.

- **Kevin Collier, *Reporter, CNN***

  Kevin Collier is a reporter who covers the intersection of cybersecurity and national security, including efforts to safeguard election integrity. He has previously worked for BuzzFeed News, Vocativ, and the Daily Dot.

- **Kim Zetter, *Longtime cybersecurity/national security reporter for various publications including WIRED, Politico and The New York Times Magazine and author of the book* Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon**

  Kim Zetter is a longtime cybersecurity and national security reporter for various publications including Wired, Politico and the New York Times Magazine and author of the book Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. She has broken numerous national stories over the years about NSA surveillance, digital warfare, Wikileaks and the hacker underground, and has been one of the nation's leading journalists covering voting machine and election security since 2003.

- **Eric Geller, *Cybersecurity Reporter, Politico***

  Eric Geller is a journalist on Politico's cybersecurity team. His primary beat consists of cyber policymaking at the White House, the Justice Department, the State Department, and the Commerce Department, but he also regularly covers election security, data breaches, malware outbreaks, and other cyber issues affecting the government, the private sector, and society at large.

While the Bots Distracted You: Hacking the Electorate

Omelas and White Ops provide the most comprehensive ever look at the day to day tactics of Russian disinformation campaigns against elections. Using Omelas' subject matter expertise and AI, we show the extent of Russian propaganda shared on Reddit in the lead up to an election, the performance of different narratives and different domains, and the sentiment expressed in articles compared to the sentiment induced in the audience in comments. White Ops's state-of- the-art bot detection demonstrates how Russia has automated the process of spreading these narratives, the added reach attributable to bots, and the techniques employed by bots.

- **Evanna Hu, *CEO and Partner, Omelas***

  Evanna Hu is CEO and Partner of Omelas and non-resident Senior Fellow at the Atlantic Council. Omelas is a cutting edge technology company that exposes imminent risks among digital data. By utilizing machine learning/ artificial intelligence and data analytics, Omelas focuses on physical threats and identifies online campaigns of adversarial state and non-state actors. Evanna is also an expert in Counter-terrorism and Countering Violent Extremism, with fieldwork in Syria, Iraq, Afghanistan, Gaza, and Sweden, working on Neo-Nazi and Islamist violent extremists.

- **Ben Dubow, *CTO and President, Omelas***

  Ben Dubow is the CTO and President of Omelas. Ben began his career tracking the online propaganda of jihadists, Shiite extremists, white supremacists, and the militia movement before joining Google where he aided YouTube in detecting ISIS content, helped to develop Project SHIELD, and provided subject matter expertise for the Redirect Method. In 2017, Ben co-founded Omelas with the mission to stop the weaponization of the internet by providing precise data and analysis on how state actors and foreign terrorist organizations manipulate the web to achieve their geopolitical goals.

Trustworthy Elections: Evidence and Dispute Resolution

Suitably designed and operated paper-based voting systems can be strongly software independent, contestable, and defensible, and they can make risk-limiting audits and evidence-based elections possible. (These terms will be defined.) Not all paper-based voting systems have these properties. Systems that rely on ballot-marking devices and voter verifiable paper audit trails produced by electronic voting machines generally do not, because they cannot provide appropriate evidence for dispute resolution, which has received scant attention. An ideal system allows voters, auditors, and election officials to provide public evidence of any problems they observe--and can provide convincing public evidence that the reported electoral outcomes are correct despite any problems that might have occurred, if they are correct.

- **Philip Stark, *Professor of Statistics and Associate Dean of Mathematical and Physical Sciences, University of California, Berkeley***

  Philip B. Stark is Professor of Statistics and Associate Dean of Mathematical and Physical Sciences at the University of California, Berkeley. He works on inference and uncertainty quantification in many applications including the census, elections, information retrieval, and Internet filters. He also studies foundational questions in the philosophy of science and statistics. He developed "risk limiting audits" as a method to check election results, which are now in law in six states and required by pending federal legislation. Stark currently serves on the Board of Advisors of the U.S. Election Assistance Commission. He has testified as an expert witness in a range of civil and criminal cases on issues including antitrust, elections, employment, equal protection, food safety, intellectual property, product liability, and vaccines.

Keynote Remarks: Senator Ron Wyden (D-OR)

- **Senator Ron Wyden**

  Senator Ron Wyden is the foremost defender of Americans' civil liberties in the U.S. Senate, and a tireless advocate for smart tech policies. Years before Edward Snowden blew the whistle on the dragnet surveillance of Americans, Wyden warned that the Patriot Act was being used in ways that would leave Americans shocked and angry, and his questioning of NSA Director James Clapper in 2013 served as a turning point in the secret surveillance of Americans' communications.

  Since then, Wyden has fought to protect Americans' privacy and security against unwanted intrusion from the government, criminals and foreign hackers alike. He has opposed the government's efforts to undermine strong encryption, proposed legislation to hold companies accountable for protecting their users' data, and authored legislation with Rand Paul to protect Americans' Fourth Amendment rights at the border.

  Wyden is a senior member of the Senate Select Committee on Intelligence and the top Democrat on the Senate Finance Committee. He lives in Portland, Oregon.

If the Voting Machines are Insecure, Let's Just Vote on Our Phones!

Despite the consensus that Russian actors targeted multiple points of U.S. election infrastructure, there are persistent calls for voting over internet-connected devices. This is not new: 31 states and

the District of Columbia allow military and overseas voters to send voted materials to their home counties via the internet, including by fax and email. Now, several jurisdictions are piloting another internet system that allows voters to send their votes via a mobile application which stores those votes in a blockchain. Such programs undermine the efforts made since 2016 to secure the election administration offices from attacks. Our military and overseas voters need to successfully cast their ballots on time – but we owe it to them to find ways that do not increase the security risk.
This talk will take a look at the current landscape of election security leading into 2020, examining the implications that technologies like blockchain could have on our elections and what the role of responsible technology looks like on our voting infrastructure.

- **Marian Schneider, *President, Verified Voting***
  Marian Schneider is the president of Verified Voting, a role to which she brings a strong grounding in the legal and constitutional elements governing voting rights and elections, as well as experience in election administration at the state level. Immediately before becoming President of Verified Voting, Marian served as Special Advisor to Pennsylvania Governor Tom Wolf on Election Policy. Previously, Governor Wolf appointed her as the Deputy Secretary for Elections and Administration in the Pennsylvania Department of State where she served from February 2015 until May 2017.
  Throughout her legal career, Marian has focused on the intersection of civil rights and election law. Formerly, she was a Senior Attorney with Advancement Project's Voter Protection program and was trial counsel in Applewhite v. Commonwealth, successfully challenging Pennsylvania's restrictive photo ID law on behalf of voters as an unconstitutional infringement on the fundamental right to vote.
  Marian received her J.D. from The George Washington University, where she was a member of the Law Review, and earned her B.A. degree cum laude from the University of Pennsylvania.

State and Local Preparations on Election Security in the Aftermath of the Mueller Report

- **Eric Geller *(moderator), Cybersecurity Reporter, Politico***
  Eric Geller is a journalist on Politico's cybersecurity team. His primary beat consists of cyber policymaking at the White House, the Justice Department, the State Department, and the Commerce Department, but he also regularly covers election security, data breaches, malware outbreaks, and other cyber issues affecting the government, the private sector, and society at large.

- **Alex Padilla, *Secretary of State of California***
  Alex Padilla was sworn in as California's Secretary of State on January 5, 2015. He is committed to modernizing the office, increasing voter registration and participation, and strengthening voting rights.
  Padilla previously served in the California State Senate from 2006 to 2014 where he chaired the Committee on Energy, Utilities, and Communications. As chair, he shepherded legislation to combat climate change and create a greener and more sustainable economy. In 1999, at the age of 26, Padilla was elected to the Los Angeles City Council to represent the same east San

Fernando Valley community where he grew up. In 2001, his colleagues elected him to the first of three terms as Council President, becoming the youngest member and the first Latino to serve in this capacity.

- **Noah Praetz, *Election Consultant; former Director of Elections, Cook County, Illinois***

  Noah is an election consultant and the former Director of Elections for Cook County, Illinois. In this capacity he was responsible for the overall management of elections in one of the largest election jurisdictions in the country.

  Noah is an adjunct professor at DePaul University College of Law teaching Election Law and sits on the advisory board of the University of Chicago Harris Cyber Policy Initiative. Noah has presented extensively on Election Security, Sustainability, Election Day Management, Voter Registration Modernization and other Election Related items. He has also published articles on cyber security, election day administration and referendum law in Illinois.

- **Barb Byrum, Ingham County Clerk, Ingham County, Michigan**

  Barb Byrum is currently in her second term as Ingham County Clerk, serving as the county's chief elections official. As Clerk of one of the most populous counties in the State of Michigan, Byrum has successfully conducted 21 elections, 4 union elections, and the 2016 Presidential Recount. Byrum currently serves on Michigan's Election Security Commission, the Secretary of State's team of advisors tasked with strengthening and better securing elections in the state.

  Byrum has been a consistent advocate for the voting rights of qualified registered voters, with a focus on voting rights of military and overseas voters. Byrum serves on the Overseas Voting Initiative, which is a joint effort by the Federal Voting Assistance Program and Council of State Governments.

  Byrum graduated from Michigan State University with a Bachelor of Science degree in agribusiness management. She also holds a law degree from the MSU College of Law. Byrum previously served three terms as a Michigan State Representative. During her time in the Legislature, Byrum served as the ranking Democrat on the House Committee on Redistricting and Elections.

- **Amber McReynolds, Executive Director, National Vote at Home Institute**

  Amber McReynolds is the Executive Director for the National Vote At Home Institute and is the former Director of Elections for the City and County of Denver, Colorado. As one of the country's leading experts on election administration and policy, she has proven that designing pro-voter policies, voter-centric processes, and implementing technical innovations will improve the voting process for all voters. During her time in Denver, the Elections office was transformed into a national and international award-winning election office. Amber was also recognized as a 2018 Top Public Official of the Year by Governing Magazine for her transformational work to improve the voting experience in Denver and across Colorado. She is now focused on improving the voting experience across the country.

2020: Ready? Or Not?

- **Sherri Ramsay, *Senior Advisor, CyberPoint International; Senior Advisor: Cyber & NSA, Cambridge Global Advisors; former Director of the National Security Agency/Central Security Service Threat Operations Center (NTOC)***

  Sherri Ramsay is a consultant, engaged in cybersecurity strategy development and planning, cyber assessments, leadership, partnership development, and marketing & development of cybersecurity tools and security operations centers.

  Ms. Ramsay is the former Director of the National Security Agency's (NSA) Threat Operations Center. She led discovery and characterization of threats to national security systems, provided situational awareness for those threats, and coordinated actionable information to counter those threats with the Department of Defense, Department of Homeland Security, and Federal Bureau of Investigation. She also served as a senior leader in NSA's Signals Intelligence Directorate, Technology Directorate, and Information Assurance Directorate.

  Ms. Ramsay holds a Bachelor of Science degree from the University of Georgia, a Master of Science Degree from Johns Hopkins University, and Master's Degree from the Industrial College of the Armed Forces, National Defense University. She is on the Board of Advisors for Virginia Tech's Hume Research Center, the University of Chicago Cyber Policy Initiative, and TruSTAR Technology.

Beyond the Voting Machine: Other High Value Targets in Today's Election System

Since the U.S. Presidential election in 2016, there has been a heightened interest in election hacking. While electronic voting machines have been the primary focus, there are other high value targets could topple our election system if they were manipulated or compromised.

Brian will share his years of research into election systems to give you an insider's view of these high value targets and how and why they could be used by an adversary. In addition to a technical analysis of the components of an electronic voting machine, he will discuss the potential weaknesses of other key pieces of today's election system that many have overlooked.

- **Brian Varner, *Special Projects Researcher, Symantec Cyber Security Services***

  Since 2010 Brian Varner has been a special projects researcher on Symantec's Cyber Security Services team, leading the company's CyberWar Games and emerging technologies development. He previously worked at the National Security Agency as a tactical analyst.

  Brian holds a bachelor's degree in Computer Science from Florida Southern and master's degree in Information Assurance from Norwich University. Since early 2016, Brian has researched electronic voting machines and campaign security issues and is often called on by peers and media for his unique perspective on the potential threats facing today's election systems.

Putting Voters First: Expanding Options to Vote

- **Amber McReynolds, *Executive Director, National Vote at Home Institute***

  Amber McReynolds is the Executive Director for the National Vote At Home Institute and is the former Director of Elections for the City and County of Denver, Colorado. As one of the country's

leading experts on election administration and policy, she has proven that designing pro-voter policies, voter-centric processes, and implementing technical innovations will improve the voting process for all voters. During her time in Denver, the Elections office was transformed into a national and international award-winning election office. Amber was also recognized as a 2018 Top Public Official of the Year by Governing Magazine for her transformational work to improve the voting experience in Denver and across Colorado. She is now focused on improving the voting experience across the country.

Thirty Years Behind the Ballot Box: A firsthand look at the multiple factors preventing fair, effective and secure elections in America

- **Ion Sancho, *former Supervisor of Elections, Leon County, Florida***

  Ion Sancho served 28 years as Supervisor of Elections of Leon County, Florida. Elected in November of 1988, Sancho was sensitized to problems in elections when 5,000 voters were disenfranchised in a 1986 state and local primary election due to the misprogramming of the voting machines. Sancho was candidate in that election, and since then has dedicated his professional career to properly administering elections in Leon County, working for fair, accessible and verifiable elections nationwide.

  Concerned by voting machine security, Supervisor Sancho sanctioned a number of red team attacks on his voting system in the spring and summer of 2005, captured in HBO's 2007 Emmy-nominated documentary "Hacking Democracy", showing how the system could be hacked to alter the outcome of any election without being detected unless the paper ballots themselves were audited.

  Ion Sancho retired after the 2016 presidential election. He has remained active in the elections field, appearing as an expert witness in election cases and working with public and private entities heightening awareness to the threat of foreign intrusion to the American voting process, particularly the critical need for audits.

UnclearBallot: Automated Ballot Image Manipulation

As paper ballots and post-election audits gain increased adoption in the United States, election technology vendors are offering products that allow jurisdictions to review ballot images---digital scans produced by optical-scan voting machines---in their post-election audit procedures. Jurisdictions including the state of Maryland rely on such image audits as an alternative to inspecting the physical paper ballots.We show that image audits can be reliably defeated by an attacker who can run malicious code on the voting machines or election management system. Using computer vision techniques, we develop an algorithm that automatically and seamlessly manipulates ballot images, moving voters' marks so that they appear to be votes for the attacker's preferred candidate. Our implementation is compatible with many widely used ballot styles, and we show that it is effective using a large corpus of ballot images from a real election. We also show that the attack can be delivered in the form of a malicious Windows scanner driver, which we test with a scanner that has been certified for use in vote tabulation by the U.S. Election Assistance Commission. These results demonstrate that post-election audits must inspect physical ballots, not merely ballot images, if they are to strongly defend against computer-based attacks on widely used voting systems.

- **Kart Kandula, *Graduate Student, University of Michigan***

  Kart Kandula received his B.S.E. degree in computer science engineering from the University of Michigan in 2019 and is currently pursuing an M.S.E in the same area. He conducts research in the UM-Security lab under the supervision of Professor J. Alex Halderman. Currently, his research interest lies in problems affecting society and public policy, specifically election security. He has held internships at Microsoft and J.P. Morgan in the past.

- **Jeremy Wink, *Undergraduate Student, University of Michigan***

  Jeremy Wink is an undergraduate student at the University of Michigan currently pursuing a BSE in Computer Science. He has taken multiple security courses and has spent time researching topics surrounding election cybersecurity under J. Alex Halderman.

Saturday, August 10, 2019

Organizational Cybernetics: A Key to Resilience for the Digital Village

- **Kimberly Young-McLear, *Assistant Professor, U.S. Coast Guard Academy***

  Lieutenant Commander Kimberly Young-McLear is currently an Assistant Professor at the U.S. Coast Guard Academy. She holds engineering and technical degrees from Florida A & M, Purdue, and The George Washington University, including a Ph.D in Systems Engineering. She has taught a breadth of courses including Operations and Project Management, Crisis Mapping & Cybernetics, and Cybersecurity Risk Management. She has been instrumental in enhancing the inclusion of cybersecurity training and education program at the Academy for cadets and faculty. Lieutenant Commander Young-McLear was a key thought leader for the development of the Coast Guard Academy's first cyber undergraduate major. Furthermore as Vice Chair, she leads a multidisciplinary faculty Cyber Council to advance cyber curriculum and research at the Academy. Her research niche is focused on protecting critical infrastructure from cyber threats in the Maritime Domain. LCDR Young-McLear is also the program developer for NET21, a middle school outreach program, designed to systematically close STEM gaps amongst underrepresented students and teachers of color in the field of cybersecurity.

Ideas Whose Time Has Come: CVD, SBOM, and SOTA

From their origins in general purpose computing, Coordinated Vulnerability Disclosure (CVD), Software Bill of Materials (SBoM), and Secure Over-The-Air (SOTA) updates have been implemented or considered in safety sectors including industrial control systems, medical device manufacturing, and ground transportation. These common software security practices are becoming widespread global norms, turning up in public policy, international standards, and national law (often in sector-specific safety regulation). This talk will briefly review the practices (what), provide examples of successful implementations and supporting information (how), and (why).

- **Katie Trimble, *Section Chief, Vulnerability Management and Coordination, U.S. Cybersecurity and Infrastructure Security Agency, Department of Homeland Security***

  Katie Trimble currently serves as the Section Chief of the Vulnerability Management and

Coordination section of the Cyber Threat & Risk Analysis (CTRA) branch of the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC). In that capacity, she leads the Department's primary operations arm for coordination of the responsible disclosure and mitigation of identified cyber vulnerabilities in control systems and enterprise hardware and software used in the 16 critical infrastructure sectors and all levels of U.S. government organizations. Ms. Trimble started her career as an intelligence analyst with the United States Air Force, specializing in counterinsurgency, antiterrorism & force protection, counter explosive devices and communications systems. Ms. Trimble holds a Bachelors of Arts in International Relations & Global Studies from Antioch University Seattle.

- **Art Manion, *Vulnerability Analysis Technical Manager, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University***

  Art Manion is the Vulnerability Analysis Technical Manager at the CERT Coordination Center, part of the Software Engineering Institute at Carnegie Mellon University. He has studied software security and coordinated responsible disclosure efforts since joining CERT in 2001. Having gaining mild notoriety for saying "Don't use Internet Explorer" and "Replace CPU hardware" in public, Manion now focuses on policy, advocacy, and rational tinkering approaches to software security, including standards development in ISO, OASIS, and FIRST. Prior to joining CERT, Manion was the Director of Network Infrastructure at Juniata College.

Incident Lifecycle and Incident Response Management Planning

In the past few years, the volume, types, and quality of cybersecurity - related attacks in elections have become more damaging and disruptive, and new types of security-related incidents have emerged. This white paper describes the best-known method for analyzing the stages of cybersecurity incidents and identifies actions that can be taken to avoid or minimize impacts at each incident lifecycle stage. We discuss the overarching workflow for elections security incident response and management and describe the Point and Line analysis approach, which considers factors such as attack vectors, motives, probability, and imp act to develop a set of Incident Response Templates in this paper. In addition, we include reusable templates for analyzing cybersecurity Incident Lifecycle and Incident Response Management, which can be customized for specific needs of any election jurisdiction in this paper.

- **Rahul K. Patel, *Elections Information Security Officer, Office of the Cook County Clerk and Chicago Board of Elections Commissioners***

  Rahul Patel is a seasoned Cyber & Information Security professional with over 25 years of experience defending the availability, confidentiality, and integrity of information assets. He is presently leading elections information security and risk management efforts at the office of the Cook County Clerk and Chicago Board of Elections Commissioners as an Elections Information Security Officer. Patel holds a PhD from Northcentral University, an M.B.A. from DePaul University, and an M.S. from Illinois Institute of Technology

- **Tonya Rice, *Director of Elections, Cook County, Illinois***

  Tonya Rice was appointed Director of Elections by Cook County Clerk Karen A. Yarbrough in 2019,

in which capacity she supports operations for one of the largest election jurisdictions in the country. Rice began her career in elections in 2005 as a political science graduate student at the University of Michigan, where she was a National Science Foundation Graduate Research Fellow, specializing in public opinion on voting technology and post-election audits, as well as the political participation of language minority citizens. Rice holds a J.D. from Northwestern University School of Law and B.A. from Northwestern University.

Assessing Election Infrastructure

- **Jason Hill, *Chief, National Cybersecurity Assessments and Technical Services (NCATS)***
  Jason Hill is the Chief of the National Cybersecurity Assessment and Technical Services (NCATS) Branch of the Cybersecurity and Infrastructure Security Agency (CISA). In this capacity Jason has primary responsibility to deliver quality security testing and analysis to customers that include the Federal government, State, Local, Tribal and Territorial governments, as well as Private Sector/Critical Infrastructure stakeholders. Mr. Hill has worked with several tech companies creating and teaching red team course work and conducting penetration testing in the commercial industry and DOD. Jason also spent 22 years as a US Army National Guardsmen for the Commonwealth of Virginia. As Master Sergeant of the 91st Cyber Brigade he led the Cyber Opposition Forces which provides red team & pen testing capabilities. He has achieved certifications for the Offensive Security Certified Professional and the Certified Ethical Hacker trainings.

- **Genevieve Marquardt, *IT Specialist, National Cybersecurity Assessments and Technical Services (NCATS)***
  Genevieve Marquardt serves as a member of the National Cybersecurity Assessments and Technical Services (NCATS) Cyber Hygiene team which is responsible for continuously assessing the "health" of external stakeholders' endpoints reachable via the internet and maintaining an updated enterprise view of the cyber security posture of their systems to drive proactive mitigation of vulnerabilities and reduce risk. Genevieve provides technical support pertaining to public IP scans and testing of .gov public facing networks for stakeholders.

- **Derrick Thornton, *Federal Lead, National Cybersecurity Assessments and Technical Services (NCATS)***
  Derrick Thornton joined the National Cybersecurity Assessments and Technical Services (NCATS) team in June 2017 as an Information Security Specialist. Derrick serves as a Federal Lead leading NCATS RVA teams conducting two week penetration tests. An 11-year veteran of the U.S. Air Force, Derrick was stationed at Robins Air Force Base, Georgia and at White Sands Missile Range, New Mexico while also serving 2 tours in the Middle East. The 4 years of military service at White Sands Missile Range was an assignment to the National Reconnaissance Office, which led to a 21-year career within the NRO. Derrick has a Bachelor of Science in Technical Management from DeVry University.

Securing America: How DHS, States, and Cybersecurity Startups are Working Together Before the 2020 Presidential Election

In 2016, 50 states' election systems were targeted by Russian nation-state hackers. Russian actors visited election websites, tested vulnerabilities by trying to exploit SQL database vulnerabilities, and even managed to access voter registration files and a county ballot. DHS deemed US election infrastructure "critical" and now CISA, DHS' critical infrastructure office, is actively providing scanning technology and technical assistance to states. States, which have direct authority over the issue, are doing a great job with their own efforts including working with the National Guard, looking public-private partnerships to provide DDoS mitigation and in some cases trying bug bounties and working with ethical hackers to keep elections secure. However, there is still much to be done to secure our democratic/election systems before 2020 - we need YOU. Election security will require a united effort with the scale and vigilance of a crowd of top talent. How are states innovating before the 2020 Presidential Election? How can hackers help?

- **Joseph Marks *(moderator), Reporter, The Washington Post***
  Joe Marks is a reporter for The Washington Post, where he writes The Cybersecurity 202 newsletter focused on the policy and politics of cybersecurity. Before joining The Washington Post, Marks covered cybersecurity for Politico and Nextgov. He also covered patent and copyright trends for Bloomberg BNA and federal litigation for Law360. Marks began his career at Midwestern newspapers covering city and county governments, crime, fires and features. He spent two years at the Grand Forks Herald in North Dakota and is originally from Iowa City.

- **Rita Gass, *CIO, California Secretary of State's Office***
  Rita established her career and progressed throughout the roles to become a chief information officer in 2008 with CCC. Remaining in this role for eight years, she eventually moved to the same role with California Secretary of State (SOS), where she continues to work now.

- **Wayne Thorley, *Deputy Secretary for Elections, Nevada Secretary of State's Office***
  Wayne Thorley is the Deputy Secretary of State for Elections for the Nevada Secretary of State's office and is responsible for administering the Nevada's election process including enforcing state and federal election laws and procedures and the Help America Vote Act.

- **Trevor Timmons, *CIO, Colorado Secretary of State's Office***
  Trevor Timmons has served the Colorado Secretary of State as Chief Information Officer since 2007, after eight years as Deputy CIO and Director of Software Development. Mr. Timmons has served under several Secretaries of State, during which time Colorado has gained a national reputation in several areas, including elections administration and cybersecurity operations.

- **Alex Joves, *Regional Director, Region V, Cybersecurity and Infrastructure Security Agency***
  Alex Joves is the Regional Director for Region V of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. He has served in various roles for DHS since 2007, including Regional Supervisor of Chemical Facility Anti-Terrorism Standards and Director of the National Infrastructure Coordinating Center. Prior to joining DHS, Mr. Joves was an

Associate Attorney at Perkins Coie LLP. He has a JD from The George Washington University Law School and a Bachelor of Science in Government from the U.S. Coast Guard Academy.

- **Josh Benaloh, *Senior Cryptographer, Microsoft Research***

  Josh Benaloh is a Senior Cryptographer at Microsoft Research and has worked on verifiable election technologies for more than thirty years. His 1987 doctoral dissertation at Yale University, entitled "Verifiable Secret-Ballot Elections", introduced the use of homomorphic encryption as a means to enable public verifiability in elections.

  Dr. Benaloh served seventeen years on the Board of Directors of the International Association for Cryptologic Research and currently serves on the Coordinating Committee of the Election Verification Network. He has published and spoken extensively and testified before Congress on election technologies and was an author of the 2018 National Academies of Science, Engineering, and Medicine report "Securing the Vote – Protecting American Democracy".

- **Alissa Starzak, *Head of Policy, Cloudflare***

  Alissa Starzak is the Head of Public Policy at Cloudflare, an Internet performance and security company that is on a mission to help build a better Internet.

- **Jay Kaplan, *Co-Founder and CEO, Synack***

  Jay co-founded Synack after serving in several security-related capacities at the Department of Defense, including the DoD's Incident Response and Red Team.

Bootstrapping Vulnerability Disclosure for Election Systems

Seven months. It look seven months to make contact with a major city after discovering a critical vulnerability in their election registration website, which could have exposed (or worse, modified) information of millions of voters. As seen in the Mueller report, election systems are under active attack by foreign adversaries. Yet while vulnerability disclosure policies are becoming the norm in most industries, exactly zero states or election vendors have established vulnerability disclosure policies to allow reporting vulnerabilities in election systems. In a time where accepting feedback from the public is the best defense against these attacks, the lack of vulnerability disclosure policies hinders improvements in securing systems. In a talk by security researcher Jack Cable and Katie Trimble from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, learn industry best practices for vulnerability disclosure and how election systems can benefit from additional public scrutiny. Hear Jack's experiences disclosing critical vulnerabilities in several major election registration systems, and how this can be channeled to protect our nation ahead of the 2020 elections.

- **Jack Cable, *Security Researcher and Student, Stanford University***

  Jack Cable is a coder turned white hat hacker and a rising sophomore at Stanford University. Jack is a top ranked hacker on the HackerOne bug bounty platform, having identified over 350 vulnerabilities in companies including Google, Facebook, Uber, Yahoo, and the U.S. Department of Defense. After placing first in the Hack the Air Force challenge, Jack began working this past summer at the Pentagon's Defense Digital Service. At Stanford, Jack studies computer science and launched Stanford's bug bounty program, one of the first in higher education.

- **Katie Trimble, *Section Chief, Vulnerability Management and Coordination, U.S. Cybersecurity and Infrastructure Security Agency, Department of Homeland Security***
  Katie Trimble currently serves as the Section Chief of the Vulnerability Management and Coordination section of the Cyber Threat & Risk Analysis (CTRA) branch of the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC). In that capacity, she leads the Department's primary operations arm for coordination of the responsible disclosure and mitigation of identified cyber vulnerabilities in control systems and enterprise hardware and software used in the 16 critical infrastructure sectors and all levels of U.S. government organizations. Ms. Trimble started her career as an intelligence analyst with the United States Air Force, specializing in counterinsurgency, antiterrorism & force protection, counter explosive devices and communications systems. Ms. Trimble holds a Bachelors of Arts in International Relations & Global Studies from Antioch University Seattle.

- **Trevor Timmons, *CIO, Colorado Secretary of State's Office***
  Trevor Timmons has served the Colorado Secretary of State as Chief Information Officer since 2007, after eight years as Deputy CIO and Director of Software Development. Mr. Timmons has served under several Secretaries of State, during which time Colorado has gained a national reputation in several areas, including elections administration and cybersecurity operations.

"The Election System: Can We Fix It?" "YES WE CAN!"

As the previous DEF CON Voting Villages have proved, our voting equipment and infrastructure are very vulnerable to multiple types of attacks. Instead of focusing on problems and broken things, this talk will focus on simple fixes that vendors and governments can put into action right now.

Starting with the machines themselves, then moving through parts of the entire system, BiaSciLab will offer suggestions on how simple practices and changes in thinking and hiring can improve the security of the entire system.

Last year at r00tz BiaSciLab was one of the first to hack the mock election reporting system set up by the Voting Village. Some have pointed out that this was a purposely flawed system designed for the the kids to break. However, as outlined in the Mueller report, Russian hackers used the same SQL injection technique to break into an election reporting system. If our systems are so secure, how was this able to happen? Lack of secure coding practices and both peer and outside review. If proper coding review and application testing had happened, this SQL injection vulnerability would have been found and fixed.

Breaking down these flaws and offering real solutions for each one, BiaSciLab will bring hope in the face of this daunting and complex security problem.

- **BiaSciLab, *Founder and CEO, Girls Who Hack***
  BiaSciLab is a 12 year old hacker and maker. She was the youngest speaker at the Hackers on Planet Earth conference and has spoken at DEF CON previously in both the Bio Hacking Village and the r00tz Asylum kids con. She received national attention when she hacked the voting reporting system at DEF CON 26. BiaSciLab is alsothe Founder and CEO of Girls Who Hack, an organization focused on teaching girls the skills of hacking so that they can change the future.

Securing Voting Systems (Beyond Paper Ballots!)

While much "headline hacking" is devoted to exposing vulnerabilities on voting machines themselves, there is more to election systems security than simply popping shells on old, unsupported kiosks. In this session, attendees will learn what real world IT personnel in the 3071 counties and parishes across the U.S. face on and around Election Day, beyond the voting machine.

- **Tod Beardsley, *Director of Research, Rapid7***

  Tod Beardsley is the Director of Research at Rapid7. He has over 30 years of hands-on security experience, stretching from in-band telephony switching to modern Internet of Things implementations. He has held IT Operations and Security positions in large organizations such as 3Com, Dell, and Westinghouse, as both an offensive and defensive practitioner.

Machine Voting: The Bulgarian Experience

First machine voting experiments in Bulgaria started in 2009. Since then machine voting found its place in legislation with the usage of offline DRE kiosks with VVPAT. Latest developments in information security and the rising threads require flexible technical approach with still lagging legislation. The talk will pass through our machine voting experience, problems and solutions we came up with. We'll share detailed security requirements for voting machines and their implementation in practice. Special emphasis will be put on latest European parliament elections, held in May 2019 and upcoming municipal elections in October 2019.

- **Alex Stanev, *CTO, Information Services JSC***

  Alex started as a software developer in late 90s working on a wide range of projects – from specialized hardware drivers to large scale information systems for private and public sectors, including e-government services, elections management and smart cities.

  Since 2003 Alex has been leading computer processing of all election results and referendum projects in Bulgaria. As a consultant for the Central Election Commission of Bulgaria Alex is the primary author of technical and security requirements for election machines used in Bulgaria. As a security consultant, Alex has lead penetration test audits in Europe, America and Africa for financial and government institutions.

  Currently Alex serves as CTO in the largest Bulgarian systems integrator - Information Services JSC.

Addressing the election security threats posed by Very Small Jurisdictions

While most election administrators in the US are working in jurisdictions with populations in the tens or hundreds of thousands, there are states with jurisdictions as small as a dozen or so voters. In these Very Small Jurisdictions, the local interface with the state election system can be as crude as a Windows XP computer directly connected to an ISP and used by an Election Administrator with little computer experience or understanding of anti-social engineering practices. These are administrators with direct user access to statewide election systems containing voter roles and responsible for posting official election results. And while there are creative approaches to improving election worker training to offset social engineering threats underway in several states, they are virtually all designed for the more typical "macro" jurisdiction level (country-level

jurisdictions) and are not scaleable to these "micro" levels, leaving secretaries of state to run generalized safety trainings with little follow-up and few options for addressing these vulnerabilities. The talk will briefly explore the threat and why creating public logical network structures are best suited not just to mitigate the problem, but to potentially make these jurisdictions even more secure than their larger counterparts.

- **John Odum, *CMC, CEH, CNDA, MCP, CIW; City Clerk, Montpelier, Vermont***
  John Odum has been the elected City Clerk of Vermont's Capital, Montpelier, for 7 years. In this capacity he also serves as the the Election Administrator for Montpelier. Prior to being elected clerk, John worked in communications and IT for non-profits and political campaigns. His work has been published on websites of The Guardian, Governing, Huffington Post, as well as numerous Vermont area publications.

The Devil Went Down to Georgia. Did He Steal Souls? (Georgia's Electronic Voting Saga)

- **Marilyn Marks, *Executive Director, Coalition for Good Governance***
  In 2009, after a narrow loss to become the Mayor of Aspen, Marilyn Marks recognized the vulnerabilities in Colorado's election systems and chose to devote herself full time to election integrity litigation and lobbying efforts for more transparent and verifiable elections. She successfully litigated the effort to make Colorado ballots open public records for postelection reviews, followed by more than 25 election-related cases involving election transparency or voter privacy. She is currently the driving force behind the legal challenge to Georgia's unverifiable electronic voting system.

- **Rich DeMillo, *Professor of Computer Science and Executive Director, Center for 21st Century Universities, Georgia Tech***
  Richard DeMillo is the Charlotte B. and Roger C. Warren Chair of Computer Science and Professor of Management at Georgia Tech, where he founded and now directs the Center for 21st Century Universities. The Center is Georgia Tech's living laboratory for fundamental change in higher education. He is responsible for educational innovation at Georgia Tech and is a national leader and spokesman in the online revolution in higher education. Under his leadership, Georgia Tech has developed a pipeline of 50 Massive Open Online Courses that together enroll a million learners.

- **Logan Lamb, *Cybersecurity researcher***
  Logan Lamb is a Senior Security Engineer at Bird. Previously he has served as a Cyber Security Researcher at Bastille Networks and Oak Ridge National Laboratory. He has Master of Science and Bachelor of Science degrees in Computer Engineering, both from the University of Tennessee, Knoxville.

- **Jordan Wilkie, *Freelance journalist covering election integrity***
  Jordan Wilkie is pursuing a career as an investigative journalist covering criminal and social justice by combining data-driven reporting with long-form, narrative storytelling. My expertise to-date is in incarcerated juvenile and LGBTQ populations.

- **Robert McGuire, *Attorney for Coalition plaintiffs***

  Robert McGuire is the attorney for the National Election Defense Coalition plaintiffs in their current legal challenge to Georgia's unverifiable electronic voting system. His previous experience includes serving as a Senior Associate at Allen & Overy LLP, as a lecturer at the University of Denver's Sturm College of Law, and as a law clerk for the U.S. Court of Appeals for the Eighth Circuit. He earned his JD from Yale Law School.

- **Susan Greenhalgh *(moderator), Vice President of Policy and Programs, National Election Defense Coalition***

  Susan Greenhalgh is Vice President for Programs at National Election Defense Coalition. Susan performs extensive research, assembling and reviewing documents that may influence and impact state and federal policy regarding election verifiability and security. She also works with cyber security experts and advisors on the federal level to bridge the gap between national cyber security policy and election administration. Susan has a bachelor's degree from the University of Vermont in chemistry.

Sunday, August 11, 2019

Exploring Voter Roll Manipulation and Fraud Detection with Voter Files

Qualified Voter Files are published by states and contain information on registered voters. These files are used by political campaigns and analysts to gather data on registered voters. The public nature of these files also makes it easier for the public to detect voter fraud and can be used by third parties to help detect large scale voter registration attacks. The data contained in these files, however, could be used by attackers to impersonate voters and update or delete a voter's registration information and subsequently prevent the targeted voters from exercising their right to vote. Use of Qualified Voter Files could also inform attackers on what scale voters' information could be changed without raising suspicion.

- **Nakul Bajaj, *High School Researcher, University of Michigan***

  Nakul Bajaj is a rising high school senior at The Harker School. He is interested in computer science and public policy, and frequently participates in hackathons and debate competitions to learning more about each of these fields. Previously, he has done analysis on election datasets, finding patterns between race and income and voter turnout. In addition, he has worked on projects dealing with a combination of law and computer science, having built an expert system that helps inventors file their own patents. This summer, he is helping conduct research in Professor J. Alex Halderman's lab at the University of Michigan regarding electronic voting machines and other election security topics with help from PhD candidate Matthew Bernhard.

Defending Democracy: Working with Election Officials to Improve Election Security

Four years after documented foreign interference in the 2016 presidential election put election security in the headlines, cybersecurity experts and election officials still face challenges in working together. The need for collaboration is clear - especially in smaller and less well-resourced jurisdictions - so how can we bridge the gap? Hear from current and former election officials and election security advocates about how successful partnerships have moved the needle, and what to do if you want to engage your local election office.

- **Liz Howard, Counsel, *Democracy Program, Brennan Center for Justice***
  Liz Howard currently serves as Counsel for the Brennan Center's Democracy Program, with a focus on cybersecurity and elections. Prior to joining the Brennan Center, Ms. Howard was Deputy Commissioner for the Virginia Department of Elections. During her tenure overseeing election modernization projects in Virginia, she coordinated the state's decertification of all paperless voting systems, implementation of the e-Motor Voter program, and adoption of online, paperless absentee ballot applications. Ms. Howard earned her J.D. from the William & Mary School of Law in 2009.

- **Justin Burns, *Chief Information Security Officer, Washington Secretary of State***
  Justin Burns joined the elections security community in January, as CISO for the Washington Secretary of State. Prior to this, he served as a Solutions Architect and Technical Assistant to the Washington State CIO.

- **Trevor Timmons, *Chief Information Officer, Colorado Secretary of State***
  Trevor Timmons became Chief Information Officer for the Colorado Secretary of State in 2007, after eight years as Deputy CIO and Director of Software Development. During this time, Mr. Timmons served under several Secretaries of State and Colorado gained a national reputation in several areas, including elections administration and cybersecurity operations.

- **Jared Dearing, *Executive Director, Kentucky State Board of Elections***
  Jared Dearing is the Executive Director of the Kentucky State Board of Elections and has worked in the elections space for over ten years. Jared has public and private sector experience working both at the local and state level, including working for the City of Louisville as well as the Office of California Governor Jerry Brown. His private sector work includes several tech startups located in the Bay Area and Boston. He is a graduate of the University of California, Berkeley where he studied public policy and engineering.

- **Monica Childers *(moderator), Product Manager for Risk-Limiting Audits, VotingWorks***
  Monica Childers is a civic technologist with a background in digital product design and project management. As Product Manager at the VotingWorks she champions collaborative design, partnering with state and local election officials to build low cost, flexible tools for election administration. Over the past decade she has designed online voter engagement platforms, vote-by-mail ballot tracking systems, text & email election reminders, and a national trouble-ticket system for reporting problems with election mail. Having served as the project manager for Colorado's post-election audit software for the past year, she is currently working with election officials implementing risk-limiting audits (RLAs) and is helping shepherd the development of nationwide RLA software.

Securing Your Election Infrastructure: Plan and Prepare to Defend Your Election Systems, People, and Processes

Robert Anderson will provide some background of Election Security and the threat research that is on-going for Election Security. An overview for election teams to plan and prepare to defend their

Election Systems, People, and Processes. Provide guidance to update your Security Policies and Incident Response Plan. Help election teams understand their Attack Surface and where your election systems are most vulnerable. Review the primary Threat Actors poised to attack your election systems. Then review several approaches that could be deployed to protect Election Security Assets, and direct to some organizations that could support election teams.

- **Robert Anderson, *Chief Cyber Security Practitioner and President, Preying Mantis***
  Robert Anderson is a highly trained IT & Cyber Security professional with over 25 years of experience in a variety of cybersecurity domains. As a former Intelligence Officer working in the Middle East, he brings a unique perspective to security operations and incident response. Robert has deployed and led over 500 security programs and projects to Fortune 500 companies, federal, state, and local governments, and NATO. Robert has over 15 years hacking experience and is a Certified Ethical Hacker. He is an expert in Cyber Threat Intelligence and Information Warfare and has led Incident Response Teams during many high-profile breaches.

Keynote Remarks: Representative Eric Swalwell (CA-15)

- **Representative Eric Swalwell (CA-15)**
  In 2012 Eric Swalwell was elected to represent California's Fifteenth Congressional District, which includes a large part of the East Bay. Now in his fourth term, he's working hard to bring new energy, ideas, and a problem-solving spirit to Congress, with a focus on advancing policies that support equality, opportunity, and security.
  Congressman Swalwell serves on the House Permanent Select Committee on Intelligence, and believes protecting Americans is Congress' most solemn duty. He chairs the Intelligence Modernization and Readiness Subcommittee, which oversees overall management of the Intelligence Community: the policies and programs focused on making sure that all 17 U.S. intelligence agencies have the workforce, infrastructure and services they need to succeed. This involves fostering greater collaboration and better use of resources across the entire Intelligence Community in personnel management, security clearance reform, information technology modernization, and other areas.

EXHIBIT D

MARICOPA COUNTY

ANALYSIS OF SENATE REVIEW

Ballots (Section 5)

The Arizona Senate issued a report on the November General Election in Maricopa County. While the County is working on a deeper analysis of the report, below is a top line review of some of the claims within the Senate's report.

CYBER NINJAS VOLUME III RESPONSES	ANALYSIS
Faulty Claim: Voted using Prior Address (Pg. 6, 14 & 16) Registered voters move, and they are legally allowed to update their addresses after the voter registration period and vote in-person or by mail. Ballots are official election mail and cannot be forwarded to another address. We have reviewed hundreds of the voter IDs provided in the referenced report's appendices and found no instances a voter illegally voted from a prior address.	23,344 ballots
Based on our preliminary review of voters found in the Senate's data, we cannot substantiate Cyber Ninjas' conclusions based on the use of a third party data set. No voter should be denied their right to vote because they are not in a commercial database. In Maricopa County, we rely on the voter's affirmation of their residential address until we are informed otherwise by the voter or by another trusted resource like the United States Postal Service or the National Change of Address report. A real-time database that tracks the day-by-day movement of every person in the state or in the nation does not exist.	2,382 ballots
Analysis: A preliminary review of voters from the Senate's data found no evidence of double voting. All voters reviewed were eligible to cast a ballot.	2,081 ballots
Faulty Claim: More Early Ballots Returned by Voters than Received (Pg. 8) All early ballots must be accompanied by a signed affidavit envelope. When returned, the envelope is scanned by the Elections Department and tracks that it was received. If the voter forgets to sign the envelope or the signature is questioned, staff works to contact the voter to "cure" the signature issue. During this process the envelope is never opened. Once the signature is "cured," the envelope is scanned again creating a subsequent "received" entry in the EV33 Early Ballot Return File. Only envelopes with verified signatures are opened and counted.	9,041 ballots
Analysis: A preliminary review of voters from the Senate's data found no evidence of double voting. These entries were related to voters legally curing questionable signatures or blank envelopes.	
Faulty Claim: Voted in Multiple Counties (Pg. 10) The Senate contractor's analysis used soft or partial matching criteria, which resulted in false duplicates statewide. Over 3.4 million registered voters participated in the November 2020 General Election in Arizona. For a true analysis, a comparison of all voter information such as full date of birth, middle name, social security and driver license numbers should have been used. As an example, included in the Senate's data are two voters with the same first and last name who live in the same home and were born in the same year. A deeper review shows they have different middle names, different social security and driver license numbers and different signatures.	5,295 ballots
Analysis: A preliminary review of voters from the Senate's data found no evidence of double voting. All voters reviewed were eligible to cast a ballot.	
Faulty Claim: Official Results Don't Include All Voters (Pg. 12 & 18) To protect the identity of judges, law enforcement officers, and victims of harassment or abuse, Maricopa County is legally required to exclude these voters from all public files, including the VM55 Voted File. This is not unique to Maricopa County. Voting jurisdictions across the nation adhere to this requirement. Maricopa County had over 3,400 protected voters participate in the November 2020 General Election.	3,432 ballots
Analysis: Voters with protected addresses are not included in public files, but are included in the official results.	1,551 ballots
Faulty Claim: More Duplicate Ballots than Original (Pg. 13) The accuracy and completeness of Maricopa County's duplication process was confirmed in court (*Ward v. Jackson*). We've again checked our detailed records, and they show 27,869 ballots were sent to duplication for the 2020 General Election. During the Cyber Ninjas' hand count, observers noted contractors spilled a box of UOCAVA ballots "across the Coliseum floor" and the large differences between the Senate's machine count and hand count have shown the faulty hand count processes to be unreliable.	2,592 ballots
Analysis: The accuracy and completeness of Maricopa County's duplication process has been confirmed by the Arizona Supreme Court.	

MARICOPA COUNTY

ANALYSIS OF SENATE REVIEW

Equipment (Section 6)

CYBER NINJAS VOLUME III RESPONSES — ANALYSIS

Faulty Claim: EMS Database & Logs Purged, Files Deleted (pg. 63, 65, 85-88)

During the November 2020 General Election, the County created daily backups of the EMS Database and Election files. These files have been maintained and safely secured. Despite claims to contrary, the Senate never subpoenaed or asked for these backup logs or archives.

> *February 2*—The County took the standard data archival steps to ready the server for certified election experts to audit the equipment, and the County was preparing for the statutorily required March 2021 jurisdictional election.
>
> *March 3*—Staff was complying with the Senate's subpoena and gathering the ballot images from the archives and tabulation equipment.
>
> *April 12*—Staff was complying with the Senate's subpoena and packing up the server for delivery.

Deleted data

Analysis: Maricopa County archived all 2020 General Election data. Two accuracy tests, a statutorily required hand count, two forensic audits from certified firms, and the Senate's machine count confirmed the ballot count was accurate.

Faulty Claim: Corrupt and Missing Ballot Images (Pg. 70 & 73)

The County provided all ballot images, pre and post adjudication, to the Senate on a two terabyte hard drive on April 22, 2021. The server and tabulation equipment are not the place to find all ballot images, as the County archived the data to ready the equipment for the statutorily required March 2021 jurisdictional election and for the audits by certified firms. These files have been maintained and safely secured. Additionally, we have since reviewed a cloned copy of the hard drive provided to the Senate and confirmed the ballot images were not corrupted and could be opened.

Corrupt & missing ballot images

Analysis: The County archived the EMS data to prepare for a statutorily required election. Ballot images were provided on a separate hard drive.

Faulty Claim: Subpoenaed Equipment Not Provided (Pg. 78)

The Senate determined the County was in full compliance with the subpoena in a settlement agreement signed on September 17, 2021. In addition, the County Ballot-on-Demand Printers (Poll Worker Laptop) and Accessible Voting Devices (ICX) were never included in any subpoena. The backup Dominion EMS Server was not used in the 2020 General Election and did not fall within the scope of the Senate's subpoena.

Not all subpoenaed equipment provided

Analysis: The County fully complied with the Senate's subpoenas, per a settlement agreement signed on September 17, 2021.

Faulty Claim: Internet Connections & Cyber Security Practices (Pg. 75-77, 89)

Maricopa County's tabulation equipment is NOT connected to the internet. The Senate's contractors misled the public, as REWEB1601 and REGIS1202 are website servers for Recorder.Maricopa.Gov. The web servers are NOT connected to the air gapped tabulation equipment. Additionally, while the tabulation equipment makes attempts to reach out to the internet for Microsoft updates, these requests fail because of the air gapped structure of the equipment. Two federally certified Voting System Testing Laboratories independently confirmed that the system is not connected to the internet.

Software & Patch Management (Pg. 75)

The equipment has the latest U.S. Election Assistance Commission approved software and patches installed. The EAC requires that any software and security updates to tabulation equipment must first be authorized by the tabulation vendor and thoroughly tested. The updates listed in the Senate presentation are part of the federally certified "trusted build" that must be installed during set up.

Connected to internet & intentionally deleted logs

Credential Management (Pg. 76)

Maricopa County has a robust set of physical security controls to prevent unauthorized access to the tabulation equipment, including controlled restricted access and security cameras. To access each tabulator, an operator needs a series of two passwords and a security token (key). Passwords used to access the election program and to tabulate ballots are changed prior to each election. Observers are present during tabulation and all totals are reconciled at the end of each shift.

Log Management (Pg. 76)

The system automatically logs all actions taken on the equipment. These logs are configured according to factory settings and have a storage limit of 20 megabytes.

Analysis: The tabulation equipment is not connected to the internet, is updated following EAC guidelines, and is configured according to factory settings. No logs were intentionally deleted.

EXHIBIT E

Cyber Ninjas
Phone: (941) 3-NINJAS
Fax: (941) 364-6527
www.CyberNinjas.com
5077 Fruitville Rd #109-421, Sarasota, FL 34232

1 Maricopa County – Analysis of Senate Review – Cyber Ninjas Response

Maricopa County continues to purposely mislead Arizonans and the American public about the nature of audit findings, and the impact they had on the 2020 General Election. Their response renames and redefines audit findings so the claim can be made that the findings are false, includes logical sounding arguments that simply don't add up, and is completely devoid of any supporting evidence. The following response to their review continues to refute their baseless claims with evidence and citations.

1.1 Voted using Prior Address (Pg. 6, 14 & 16)

The County stated that the US Postal Services National Change of Address (NCOA) should have been used as a trusted source. Melissa utilizes the NCOA for their move data. Melissa is a trusted source. This is clearly documented within the report within the respective findings and ignored by the County's response. This validates the audit results.

The lack of precision from the County's response also leaves a lot in question. Our report provides in the appendixes a full list of every voter ID affected, as well as details as to when and where that individual moved. The County's response doesn't even confirm an exact number of records that were validated, nor the explanation for why the records they validated were not an issue. The County expects that simply asserting that our claim is false makes it false, rather than providing any documentation to validate their claims.

Furthermore, the County's claim that voters can legally change their addresses after the voter registration period and still legally vote is an extremely misleading statement. Our report was primarily[1] based on the November 7th VM34 voter roll file, and therefore any address changes should have been reflected in that version of the file. In addition, this is only possibly applicable for individuals who move within Maricopa County (15,035) and would not apply to individuals who moved outside of the County (12,772) and would therefore be required to re-register to vote. It would also be expected that the County would be able to state exactly how many of the 15,035 changed their address, rather than making a blanket statement and implying that it fully explains the finding. The fact the County chose not to do this raises more questions.

It is also unclear why the analysis in the County's response for this finding talks about double-voters. This finding has nothing to do with double voters.

1.1.1 Mail-in Ballots Voted from Prior Address

On Twitter, the County suggested that the largest of our findings associated with a change in address was inaccurate because it didn't take into account college students, snowbirds, or military personnel. The County did not read the report very carefully if it believes that college students and snowbirds could significantly impact these numbers. The finding very clearly states that the address was checked after the documented move date and if anyone was still at the residence with the same last name the voter ID was removed from the list. This should account for almost all situations with college student and snowbirds.

[1] Please see page 20 of the Maricopa County Forensic Election Audit Volume III: Results Details report for additional details: https://c692f527-da75-4c86-b5d1-8b3d5d4d5b43.filesusr.com/ugd/2f3470_d36cb5eaca56435d84171b4fe7ee6919.pdf

The question of military personnel is potentially a legitimate partial answer. The voter rolls clearly delineate military personnel by specifying a military address, as well as frequently having eligibility for voting via the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA). While the former is less likely to impact the numbers for the same reasons as the college students and snowbirds; UOCAVA eligible voters can vote via email, fax, or a portal in addition to via mail and it shows up as a mail-in vote. As a result, they would not necessarily have to have access to their prior residence address to receive their ballot in order to cast a mail-in-ballot. Running the 23,344 voter IDs who voted via mail-in ballots even though they had moved against a list of UOCAVA eligible voters finds 1,344 UOCAVA voters. This means the proper count for the first finding in our report should be an even 22,000.

1.2 More Early Ballots Returned by Voters Than Received

The numbers simply do not support the County's claim that the curing of ballots would result in a second scanning of the envelope, and therefore a second EV33 entry for a received ballot. This is a soundbite, not an explanation.

The 9,041 voter IDs that had more EV33 returned ballot entries than EV32 sent ballots, and the individual voted via mail was provided to Dr. Shiva to see if there was any correlation between these voter IDs and the prevalence of more than one scanned envelop. Only 2,138 of these voter IDs had more than one scanned ballot. If the County's explanation properly accounted for this issue, then there should be a one-for-one match with multiple scanned ballots for all 9,041 voter IDs. This simply cannot explain the issue when only 24% of the 9,041 had multiple envelop image scans.

1.3 Voters That Potentially Voted in Multiple Counties

It does not appear the County read the report carefully. The finding is extremely clear that the list of identified individuals should be validated further as name and birthdate overlaps can occur and be shared by different people. The County has access to full social security numbers and driver's license numbers. The audit does not. It is not uncommon nor improper for an audit to find things that require additional investigation, and we look forward to the Attorney General's review of this finding rather than the County's cursory dismissal of this issue as a "Faulty Claim".

Had the County taken this finding seriously their reply could have shown a good faith effort to validate the finding and indicate the quantity validated and the reasons why they were not valid. Without any numbers or evidence, it can only be assumed that the County completely dismissed this, as stated, as a "Faulty Claim".

NOTE: The County renamed this finding in their response to take out the word "Potentially" so it could be listed as a faulty claim, rather than recognized the validity of the finding.

1.4 Official Results Does Not Match Who Voted

This finding is accurate as written. The Official Results from the Canvass do not match the list of voters in the VM55 file. The County attempted to conceal this flaw by renaming this finding in their response to "Official Results Don't Include All Voters" for the sole purpose of falsely discrediting the claim. Their explanation states that protected voters are not included in the VM55 file and therefore there is a discrepancy. This does not explain the issued raised by the audit team; the fact the County couldn't reply with a precise number of protected voters who voted in the election that matches the outlined discrepancy shows that their response is not accurate and willingness to address flaws in their system is non-existent.

Furthermore, several weeks before the hearing the Senate attorney reached out to the County to request an explanation for this so that it could be ensured that the audit report was as accurate as possible. The County ignored the request for weeks and then replied to the request the night before the hearing with the details about the protected voters list. To ensure the accuracy of our audit despite the County's willful lack of cooperation, we both discussed this possible explanation in the hearing and included disclaimers in the report for findings that would be invalid if this information was true.

1.5 More Duplicate Ballots than Original

The County's response is extremely misleading and does not respond to any of the specific details outlined within the audit report. In the case cited by the County, Ward vs. Jackson, only 1,626 ballots were reviewed, while the audit reviewed all of the duplicated ballots[2]. The "spilled box of UOCAVA ballots" referenced in the County's response was not a box, but a stack of 20. That stack of 20 slide onto the ground in a manner that even maintained the order of the ballots; and was promptly picked up and put back in the box. This occurred within the contained space of the Senate's special ballot coral under the direct view of Ken Bennett and the Secretary of State observer, Ken. This doesn't account for anything close to the discrepancies detected by the audit.

Furthermore, the "detailed records" provided by the County for duplicate ballots were shown by the audit to be incorrect and full of mislabeling and other errors as documented in the report. Detailed records are only useful if they're correctly recorded.

1.6 EMS Database & Logs Purged, Files Deleted

The County's response to the purged and deleted data and files shows they do not know what is going on within their Election Management System (EMS), and that they didn't carefully read the subpoena. Not only are many of the items that were deleted specifically listed in the original subpoena, and therefore a request for an archive or backup wouldn't be needed; but the dates and timelines in their response to the audit report and on Twitter is not supported by the dates in the logs on the machines. Furthermore, what was done for the November 2020 general election does not match any past elections found on the EMS Server; countering any arguments that the purging and deletion of files is "standard procedure", and the over 2 terabytes of free storage on the device counters any arguments it had to be done for space. These arguments are handled in the following sections but show clear evidence that data that should have been protected by the subpoena was instead destroyed.

1.6.1 False County Claim: The Senate Needed to Subpoena Backups or Archives

The Senate did not need to subpoena backups or archives. All disputed items were clearly outlined within the Senate, this is nothing more than an attempt to misdirect and mislead. The original subpoena[3] item #4 clearly requests the "November 2020 general election in Maricopa County, Arizona", "Election Log Files" and "any other election files and logs", and it goes on to list "any other election files or logs" associated with the "Tabulators", "Result Pair Resolution", "Result Files", and "SQL Database Files". DVD result files and SQL database files are among the list of items deleted.

---

[2] https://recorder.maricopa.gov/justthefacts/courtcases/7%20Ward%20v.%20Jackson%20(AZ%20Supreme%20Court)/Ward%20v.%20Jackson%20APPEAL%20-%202020.12.08%20DECISION%20ORDER%20(Ward%20v.%20Jackson,%20Ariz.%20S.%20Ct.).pdf (pg. 4)

[3] https://www.scribd.com/document/531671852/SUBPOENA-January-12-2021-NEW-Senate-Sub-to-Maricopa-County

In addition, at the point where the SQL Database was purged of all data associated with the results of the November 2020 general election and later filled with audit data from ProV&V, it no longer would be a file reflective of the "November 2020 general election"; but would be a file that represented the ProV&V "audit". This would mean it would not meet the requirement from the subpoena for the SQL Database files associated with the election.

Furthermore, the original subpoena[4] item #7 clearly requests the "November 2020 general election in Maricopa County, Arizona", all "Windows Server & Desktop" "Windows event logs and Access logs". The Security event logs were not provided separately for any of the systems; even though this is the definition of what an "Access Log" is for a "Windows Server & Desktop". Since these logs were rolled over prior to us receiving the machine, they no longer covered the subpoenaed period of time.

1.6.2 False County Claim: Standard Archival Steps Were Taken on February 2nd.

The Results Tallying and Reporting (RTR) logs clearly show that all database data as well as files in the NAS directory were purged and deleted on February 1st. The action was started at 5:14:47 pm and finished at 5:20:00 pm. If any backups or archives were conducted on February 2nd, the data was already deleted.

userRelatedInfo	executedCommand	operationTimestamp
RTRAdmin	User initiates the OnPurgeResults activity	2021-02-01 17:14:47.363
RTRAdmin	PurgeResultsCommand (execution duration: 76478ms):All result files from database were deleted.	2021-02-01 17:16:27.810
RTRAdmin	PurgeResultsCommand (execution duration: 288779ms):The result files database, result files and images from NAS were deleted. Purging of results has finished successfully.	2021-02-01 17:20:00.097

If it was normal to purge data as can be seen in the finding in the audit report, it would be expected that this would be true for every other election on the EMS Server. However, as can be seen in the screenshots below the data is still present for other past elections. Since the drive had more than 2 terabytes of free space available there was no technical reason to delete the data before the two audits hired by Maricopa County. In fact, it begs to question what the auditors had to audit if there were no election results when ProV&V arrived on Feb 2nd.

[4] https://www.scribd.com/document/531671852/SUBPOENA-January-12-2021-NEW-Senate-Sub-to-Maricopa-County

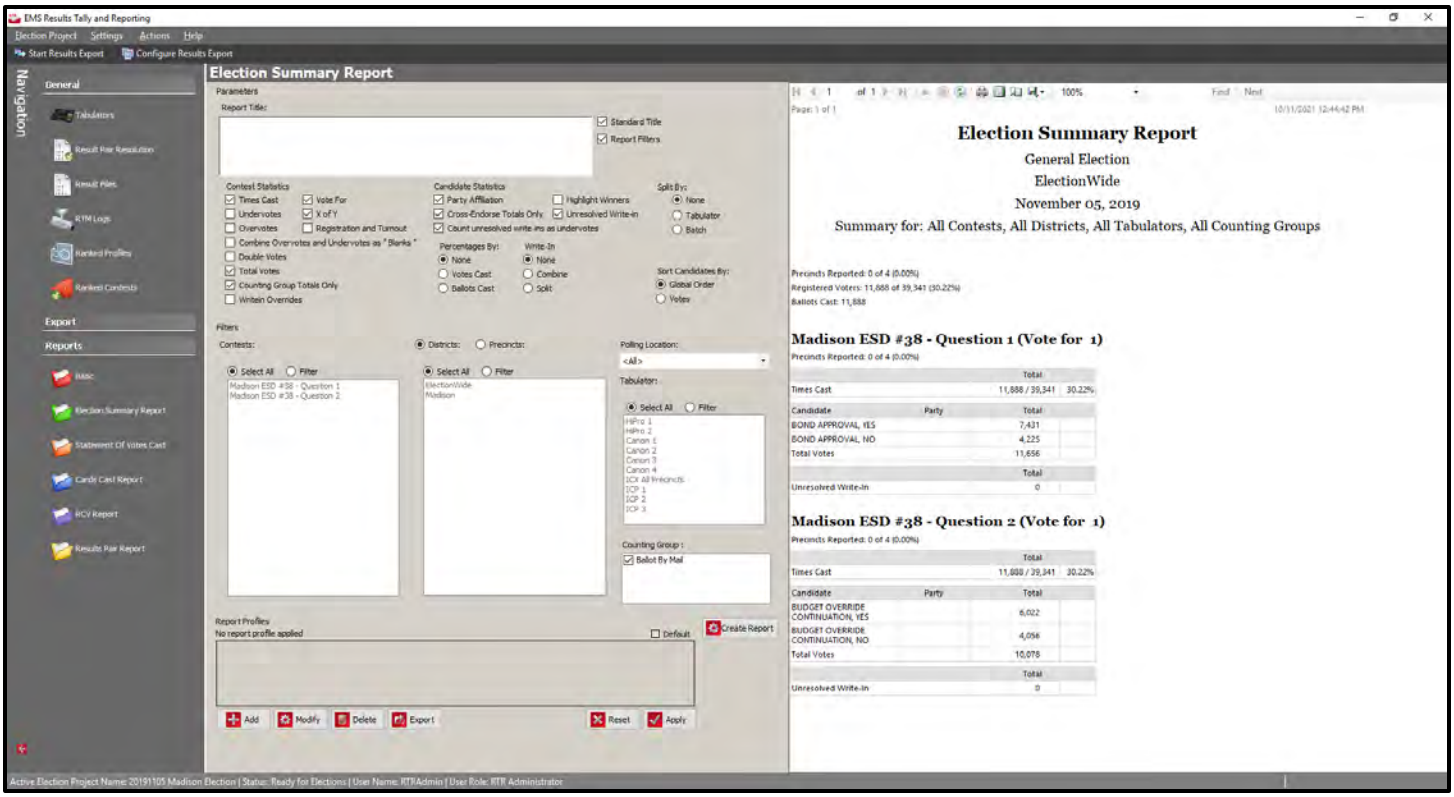


Figure 1 - Election Results for the 2019 Madison Election. These numbers match the Official Results on the Recorder's Site.

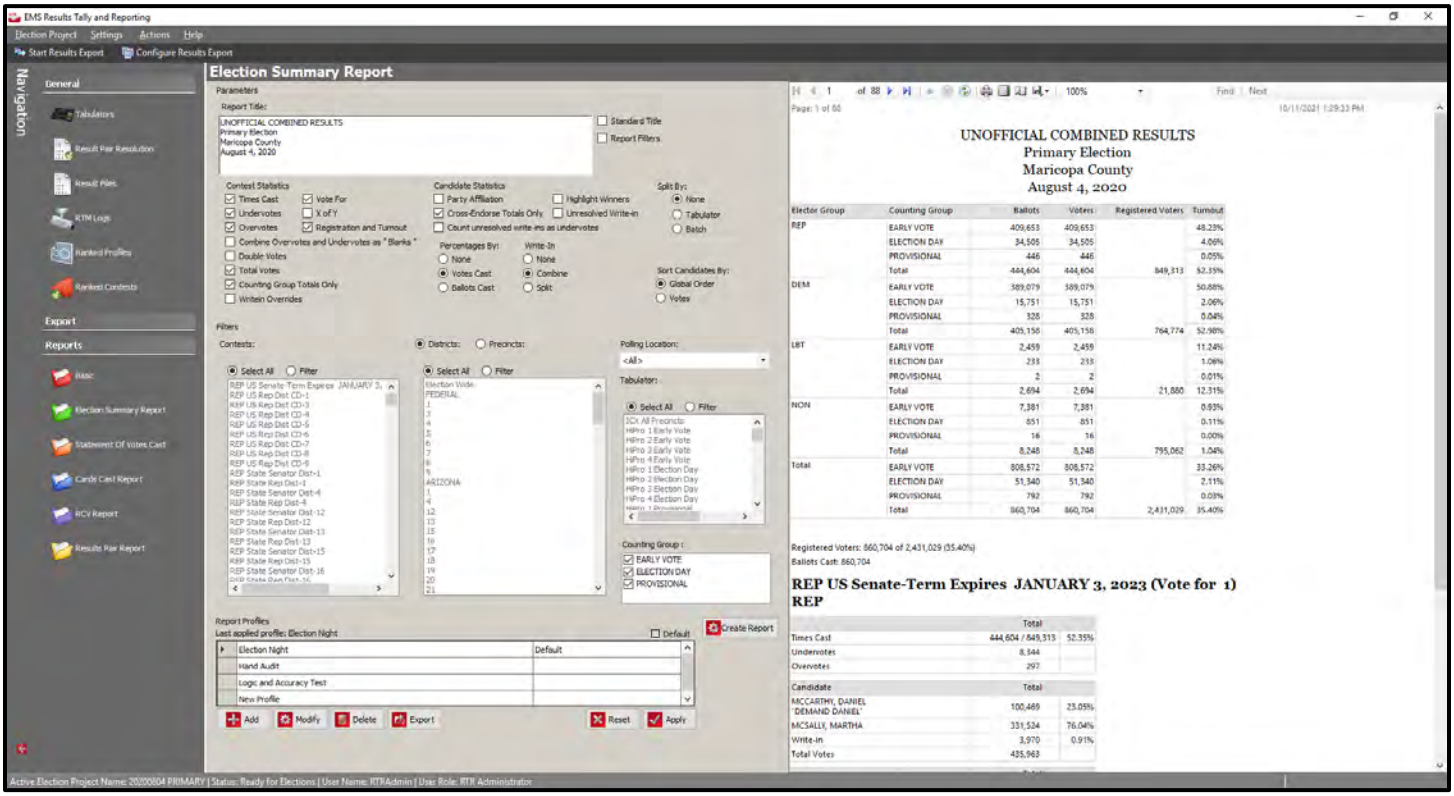


Figure 2 - All Results Still Exist for the 2020 Primary. These numbers match the Official Results.

Furthermore, the standard way to "archive" Dominion software is to run a backup from Election Event Designer. This method of backup is found with every past election, and it's the only way to create a zip archive with all of the database details and all of the items within the NAS directory. This operation does NOT delete any data. The last time a package file was created was on November 13th as can be seen in the screenshot of the RTR logs. This is inconsistent with the County's statement an archive was created on Feb 2nd.

Results | Messages

	userRelatedInfo	executedCommand	operationTimestamp
1	Admin	User initiates the Create backup... activity	2020-11-13 16:28:32.560
2	Admin	User initiates the Create backup... activity	2020-11-12 21:07:53.480
3	Admin	User initiates the Create backup... activity	2020-11-11 20:49:44.793
4	Admin	User initiates the Create backup... activity	2020-11-10 20:46:11.193
5	Admin	User initiates the Create backup... activity	2020-11-09 18:20:26.423
6	Admin	User initiates the Create backup... activity	2020-11-07 21:58:32.450
7	Admin	User initiates the Create backup... activity	2020-11-06 22:55:52.387
8	Admin	User initiates the Create backup... activity	2020-11-06 00:42:47.217
9	Admin	User initiates the Create backup... activity	2020-11-05 01:14:35.003
10	Admin	User initiates the Create backup... activity	2020-11-04 02:22:22.277
11	Admin	User initiates the Create backup... activity	2020-11-03 19:05:35.677
12	Admin	User initiates the Create backup... activity	2020-11-03 00:47:26.613
13	Admin	User initiates the Create backup... activity	2020-11-01 23:15:09.207
14	Admin	User initiates the Create backup... activity	2020-10-31 23:58:44.483
15	Admin	User initiates the Create backup... activity	2020-10-31 00:29:48.753
16	Admin	User initiates the Create backup... activity	2020-10-30 00:20:37.450
17	Admin	User initiates the Create backup... activity	2020-10-29 00:06:04.167
18	Admin	User initiates the Create backup... activity	2020-10-27 20:52:48.840
19	Admin	User initiates the Create backup... activity	2020-10-26 18:51:58.773

Figure 3 - The last time an archive was created of the 2020 General Election was on 11/13 at 4:28pm.

1.6.3 False County Claim: The County Ran Two Forensic Audits By Certified Companies

The procedures documented within the ProV&V report for the first Maricopa County audit did not follow any industry recognized standard digital forensic processes, and the SLI report clearly documents that they could not forensically image the EMS Server due to the RAID configuration. This is consistent with the fact that neither company is certified for forensic examination of digital equipment, and this is not work either company regularly does. Both companies are certified by the Election Assistance Commission for certifying election equipment, not for completing forensic audits.

Furthermore, since all election results were cleared from the Election Management System (EMS) Server before any of these two audits were performed; the only thing these companies could do was run test cases against the election equipment to see if it behaved properly. No results were audited by either of these two companies.

1.6.4 Misleading County Claim: The County Ran A Hand Count

The hand count done by Maricopa County was such a small sample size that its margin of error was more than twice the amount of the margin of victory. It is extremely misleading to suggest this is equivalent or just as accurate as a full hand count. The hand count only counted 5,200 of the 2,089,563 ballots. This equates to roughly 1/4th of a percentage point of the total ballots. With this small sample size there would be a 1.357% margin of error to achieve a 95% confidence in the election results. This means that if the ballots were truly chosen randomly, then this hand count could be off by over 28,000 ballots. If the ballots were not chosen randomly then the counts could be off by even more.

1.7 Corrupt and Missing Ballot Images

The County claims that the fact that the ballot images are corrupt or missing from the Election Management System (EMS) Server is inconsequential, and that ballot images should have been viewed from one of the other drives provided. This defies normal audit principles where the official system of record, the EMS Server, would be utilized for the analysis. This also doesn't explain why or how the images got corrupt, or why images are missing from that system. The drive provided wasn't even in the same folder structure as the NAS directory or have any other resemblance of an official backup. For this drive to be considered as the official source of images would require that there is some documented procedure for the collection of these images.

Furthermore, a review of the drive provided doesn't include all pre-adjudicated images. The post-adjudicated images on the drive show the expected 2,089,563 images, but the pre-adjudicated images only show 1,923,719 images. The difference of 165,844 appears to be the number of ballots processed by the Election Day ImageCast Precinct 2 tabulators based on the CVR, but it's unclear why or how these images would be collected in a manner where these images were missing. As a result, it creates further questions on the reliability of these images.

At this time, the drive of pre- and post-adjudicated images has not been validated to confirm that corrupt images do not exist, but this aspect will be reviewed and be confirmed.

1.8 Subpoenaed Equipment Not Provided

The County can't both state that the matter of missing subpoena items was resolved in the settlement, and then proceed to argue that certain items were not in the subpoena. Furthermore, failing to comply with a subpoena is a criminal offense and not something that can be included in a civil settlement. It will be up to the Attorney General to determine if the missing subpoena items are a sufficient grievance to merit further investigation or prosecution. This is not something that is within the Senate's responsibilities.

The actual report has a more extensive list of items that were missing from the subpoena, not all of which are addressed within the County's reply. However, to address the specific items listed in the County's reply:

- **Poll Worker Laptops / Sitebook Voter Roll Check-In Devices**
  - Item #11 on the original subpoena[5] states, "forensic image of computers/devices used to work with voter rolls". This was not provided.
- **Backup Dominion EMS Server**
  - The county states that the Backup Dominion EMS Server was not in use. Logs show regular backups conducted of the election database throughout the election. Normal practices would dictate that these would periodically be loaded onto a backup server to confirm the backups integrity. By definition, this is how a backup server is used and it was part of the election.
  - Item #3 on the original subpoena[6] states, "For the November 2020 general election in Maricopa County, Arizona", "Hardware and Forensic Images of Election Servers…". The backup EMS Server was not provided.
- **Ballot-on-Demand Printers & Accessible Voting Devices (ICX)**

[5] https://www.scribd.com/document/531671852/SUBPOENA-January-12-2021-NEW-Senate-Sub-to-Maricopa-County
[6] https://www.scribd.com/document/531671852/SUBPOENA-January-12-2021-NEW-Senate-Sub-to-Maricopa-County

- Item #1 of the original subpoena[7] states "The ballot tabulation and processing equipment from each polling place and tabulation center".
  - Based on the sentence "processing equipment" that is different than "ballot tabulation". It's unclear what else this could be referring to besides Ballot-on-Demand Printers and accessibility Ballot Marking Devices since those are the only other devices that process ballots at a polling location.
- Item #10 of the original subpoena[8] states "Election Systems and Software", "Ballot on Demand – BOD printing system":

1.9 Internet Connections & Cyber Security practices

The County continues to repeat the claims that there was no way any of the systems could access the internet, to abdicate all responsibility to other parties for the County's failure to properly maintain the security of election systems, and to purposely misdirect on all other legitimate findings of the audit. As usual, the County fails to cite a single piece of evidence to support their opinion.

1.9.1 Internet Connectivity

The County's response does not state that the systems were never connected to the internet; but always seems to address this issue in the present tense indicating that the election system is not currently connected to the internet; and then cite the two "forensic audits" conducted by the County that proved at the time of their "audits" there was no evidence of internet activity. CyFIR's analysis never stated that the systems were always connected to the internet, but simply stated that there are distinct periods of time where internet connectivity can be validated. As a result, while on the surface it looks like the County is countering the claims in the audit report; in fact, their response appears to be a misdirection.

CyFIR utilized a tool called HstEx v4 from Digital Detective to review the hard drives of all the affected systems for artifacts of internet activity. This tool both looks at the allocated space, which is the normal file structure you see on a system, and the unallocated space, which is what shows up on your system as "free space". When you delete a file on your file system the space that file occupied is shown in the computer as "free space"; but the file itself is still fully intact on the file system until the computer puts some other file in the space occupied prior by that file. In this way the tool looks at both normal files and deleted files.

HstEX v4 identified and extracted all internet history into a .hstx file that was analyzed using the Digital Detective NetAnalysis v2 tool. In addition to the URL that was navigated to, this data includes a visits column. Per the tool documentation[9] and basic forensic analysis, the visits field is ONLY populated when a URL is actually visited and does not populate when a web page cannot be resolved. This visits column can be seen in all of the following screenshots of the tool output, and clearly refutes the claim that the machines never had a pathway to the internet.

[7] https://www.scribd.com/document/531671852/SUBPOENA-January-12-2021-NEW-Senate-Sub-to-Maricopa-County
[8] https://www.scribd.com/document/531671852/SUBPOENA-January-12-2021-NEW-Senate-Sub-to-Maricopa-County
[9] https://www.digital-detective.net/Documents/NetAnalysis%20v2%20User%20Guide.pdf

1.9.1.1 EMS SERVER CONNECTIONS

On 2 February 2021 the EMS Server connected to the az700632.vo.msecnd.net web site three times.

Date Visited [UTC]	Date Visited [Local]	Visits	URL
2021-02-02 00:17:30.906	2021-02-01 17:17:30.906	1	https://az700632.vo.msecnd.net/pub/ExtMgr/CompatList/CompatibilityList.xml.errormarker
2021-02-02 00:17:33.935	2021-02-01 17:17:33.935	2	https://az700632.vo.msecnd.net/pub/ExtMgr/CompatList/CompatibilityList.xml.errormarker

Figure 4 - EMS Internet Connections

1.9.1.1 EMS CLIENT 1 CONNECTIONS

The EMS Client 1 connected to three different sites a total of 9 separate times after the installation of the Dominion software. Figure 5 – EMS Client 1 Connections details these connections.

Date Visited [UTC]	Date Visited [Local]	Visits	URL	User
02/07/2020 20:02:19	02/07/2020 13:02:19	2	http://www.bing.com/search?q=192.138.100.11&src=IE-SearchBox&FORM=IE11SR&pc=EUPP_	
02/22/2021 23:08:13	02/22/2021 16:08:13	5	https://go.microsoft.com/fwlink/?LinkId=838604	emsadmin01
02/07/2020 20:00:53	02/07/2020 13:00:53	2	https://go.microsoft.com/fwlink/p/?LinkId=255141	emsadmin01

Figure 5 - EMS Client 1 Connections

1.9.1.2 EMS CLIENT 3 CONNECTIONS

The EMS Client 3 connected to the go.microsoft.com web site 6 times after the installation of the Dominion software. Figure 6 – EMS Client 3 Connections details these connections.

Date Visited [UTC]	Date Visited [Local]	Visits	URL	User
08/06/2019 16:26:03	08/06/2019 09:26:03	2	http://192.168.100.11/portal_top.html	emsadmin01
08/06/2019 16:26:01	08/06/2019 09:26:01	2	http://192.168.100.11/	emsadmin01
08/06/2019 16:26:03	08/06/2019 09:26:03	2	http://192.168.100.11/portal_top.html	emsadmin01
08/06/2019 16:26:03	08/06/2019 09:26:03	2	http://192.168.100.11/portal_top.html	emsadmin01
08/06/2019 16:26:01	08/06/2019 09:26:01	2	http://192.168.100.11/	emsadmin01
08/06/2019 16:26:13	08/06/2019 09:26:13	3	http://192.168.100.11/	emsadmin01
08/06/2019 16:26:27	08/06/2019 09:26:27	3	http://192.168.100.11/checkLogin.cgi	emsadmin01
08/06/2019 16:26:27	08/06/2019 09:26:27	3	http://192.168.100.11/portal_top.html	emsadmin01
02/04/2021 00:36:19	02/03/2021 17:36:19	6	https://go.microsoft.com/fwlink/?LinkId=838604	emsadmin03

Figure 6 - EMS Client 3 Connections

1.9.1.3 REWEB1601 AND REGIS1202 CONNECTIONS

The Maricopa County Board of Supervisors represented to the public and to the auditors that none of the election systems were connected to the internet. The Maricopa Board of Supervisors did not provide any qualifying statements to the auditors at the time of equipment delivery, nor did they provide a network diagram explaining that the REWEB1601 and the REGIS1202 servers were connected to the internet. The auditors subsequently took the Maricopa Board of Supervisors at their stated word and reported the internet connections to each of these servers to the Arizona Senate. The auditors appreciate the Maricopa County Board of Supervisors admission that these two servers were indeed connected to the internet. The Maricopa County Board of Supervisors stated that two federally certified Voting System Testing Laboratories independently reported that the systems were not connected to the internet. It is not uncommon for firms to miss internet artifacts that may exist in the unallocated and allocated space of a system.

1.9.2 Software and Patch Management

The County's neglect of the software, patch management, and virus scan updates violates all solid principles of Cyber Security and demonstrates a negligence in protecting the integrity of voting system. Their attempts to blame the Election Assistance Commission (EAC) is disingenuous at best and simply demonstrates they're failure to take responsibility and control of their election systems, and instead attempting to delegate all responsibility to the voting machine vendor.

The EAC clearly has a process for "de minimis changes"[10] to account for Operating System level patches and changes to trusted builds, and advocates those critical patches be applied[11]. This advice is further enforced by the Cybersecurity & Infrastructure Security Agency[12] (CISA), and the Center for Internet Security[13] (CIS). Nowhere in any documentation is there any indication that virus scans update would somehow negate the certification, yet those were also not applied.

The fact that the County failed to recognize the risk of having out-of-date software and never requested the voting machine vendor to go through the simple process to get patches approved, as is required by the "Warranty" section of the County's contract[14], nor did they choose to move to a later version of the voting system software that has later approved patches; does not somehow make their system secure. The County failed to implement basic Cybersecurity hygiene. This should be acknowledged, and policies put in place to make sure this never happens again.

1.9.3 Credential Management

The County's response related to credential management is beyond misleading and goes into the realm out outright lies. They state, "To access each tabulator, an operator needs a series of two passwords and a security token (key). Passwords used to access the election program and to tabulate ballots are changed prior to each election." This statement only applies to the ImageCast Precinct 2 (ICP2) tabulators which were ONLY used on election day and doesn't apply to ballots tabulated on the HiPro or the ImageCast Precinct devices. To give perspective, the ICP2 only accounted for 7.9% of the vote, while the other tabulators accounted for 92.1% of the vote. The devices that tabulated 92.1% of the vote, as well as the systems utilized to generate the output for the official certified results; were where the problems outlined within the audit report were found.

To be more specific, the credential management finding is specific to the username and passwords required to access the EMS server, the EMS workstations, the Adjudication workstations, the HiPro scanners and the ImageCast (ICC) Workstations. Accessing these systems did not require anything but a typical computer username and password combination. The usernames/accounts of these systems were not assigned to specific individuals, but rather were shared between various people. The passwords for these accounts were created during the installation of the Dominion software on 8/6/2019 and were never changed up to the point where these systems were delivered for the audit. Furthermore, in complete disregard to all standard security practices, the same password was used for ALL user accounts on ALL of the EMS, EMS Client, ICC, HiPro, and Adjudication systems. To be clear, if someone knew the password to a single user account on one of these systems that individual would know the password to the admin account on any of these systems.

---

[10] https://www.eac.gov/sites/default/files/voting_equipment/NOC19.01_SoftwareDeMinimisChanges_11-15-2019.pdf
[11] https://www.eac.gov/windows-critical-update-faq
[12] https://us-cert.cisa.gov/ncas/tips/ST19-002
[13] https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-patching/
[14] https://www.scribd.com/document/533751776/Maricopa-County-Elections-Tabulation-System-Contract (Page 34)

1.9.4 Log Management

The Maricopa County Board of Supervisors stated the following in response to the Audit report concerning the County's failure to preserve the operating logs on the EMS server "The system automatically logs all actions taken on the equipment. These logs are configured according to factory settings and have a storage limit of 20 megabytes." This statement ignores the crux of the finding.

1.9.4.1 Failure to Properly Retain Logged Data

Maricopa county had full administrative authorities over the configuration and maintenance of the logging functions and the log retention duration operations. To claim that the reason the log data was not retained because the log size default setting was only 20MB is disingenuous at best when the county had the full control to properly modify this setting to ensure that the logged data was properly retained. The retention period for these log artifacts should have been for twenty-two (22) months but wasn't.

1.9.4.2 Intentional Execution of Scripts to Deliberately Ensure that Log Entries Were not Retained

The response by Maricopa County does not address the fact that a user leveraging the emsadmin account deliberately and purposely executed a script that checked the accounts for duplicate passwords 38,478 times. This deliberate execution of the script occurred over three days, specifically on 2/11/2021 there were 462 log entries overwritten, on 3/3/2021 there were 37,686 log entries overwritten, and on 4/12/2021 there were 330 log entries overwritten. Given that the Maricopa County knew that the setting on the log retention was limited to 20MB, the act of executing these scripts had the effect of deliberated ensuring that the Windows security logs covering the dates of the general election would not be available for review.