ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Hacking Elections is Easy!

Part 2: Psst! Wanna Buy a National Voter Database? Hacking E-Voting Systems Was Just the Beginning

September 2016

Authors

James Scott (Senior Fellow – Institute for Critical Infrastructure Technology)

Drew Spaniel (Researcher – Institute for Critical Infrastructure Technology)

Thought Leadership Contributions from the Following Experts:

Jim Walter (ICIT Contributor & SPEAR Researcher, Cylance)

ICIT Briefing: Hacking Elections is Easy!

October 20, 2016

Washington D.C.

Join ICIT experts in a briefing on its two-part research series on vulnerabilities in electronic voting.

http://icitech.org/event/hacking-elections/

Related Research

Hacking Elections is Easy! Part One: Tactics, Techniques, and Procedures **-** http://icitech.org/icit-analysis-hacking-elections-is-easy-part-one-tactics-techniques-and-procedures/

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Contents

Introduction

Western democracy is held hostage to vulnerable code in black boxes on dilapidated bare bones PCs with virtually zero endpoint security, otherwise known as e-voting machines. Moreover, the systems are maintained and managed either by manufacturer personnel who obfuscate the insecurity of the systems or by local and state voting officials who are the very prototype of victims that repeatedly fall for spear phishing, ransomware and malware attacks and other easily avoidable cyber-attacks. The problem in the sector is not merely a matter of lacking basic cyber hygiene, rather it is the sheer absence of the technical aptitude required to understand the cyber, physical and technical landscape available for exploit by the multitude of adversaries possessing a keen interest in manipulating the election process. As expressed in *Hacking Elections is Easy! Part 1: Tactics, Techniques, and Procedures*, a complete overhaul in the extensively vulnerable election process needs to be at the forefront of the conversation when it comes to securing the legitimacy of our democracy. In this report, the vulnerabilities of individual electronic voting machines will be briefly enumerated as a demonstration of how every major electronic voting system is utterly devoid of security and transparency operations. While it is possible that some of the vulnerabilities discussed in this report are mitigated on some machines, it is difficult to assess whether or not the black-box systems have been updated or patched by the manufacturers. At the local and state levels, updating and patching is less likely because personnel lack any form of cybersecurity training and awareness. Therefore, it is unlikely that the threat landscape surrounding electronic voting machines has decreased over the past decade. In all likelihood, the opportunity to exploit a vulnerable machine continues to increase as the electronic voting machines age and become more interconnected with networked machines and more accessible and exploitable to unsophisticated attackers.

Manufacturers

The United States election process has been at risk since the widespread adoption of electronic voting (e-voting) systems in 2002-2006. Electronic voting manufacturers operate without sufficient accountability, oversight, and governance. Rather than produce robust, secure systems, they distribute bare bones proprietary systems with less native security than a cheap cell phone. Security researchers have enumerated countless exploitable vulnerabilities in the proprietary black-box e-voting systems that have been manufactured with limited native security and little transparency, accountability or cyber-hygiene.

Despite uncovering hundreds of attack vectors and exploitable vulnerabilities in the 36 antiquated and ill-maintained proprietary e-voting systems currently in use in the United States over the last decade, it is likely that researchers have only discovered a portion of the attack landscape. In many cases, it is unclear whether the vulnerabilities discovered by researchers are ever patched or mitigated in these systems because manufacturers have only limited accountability and less transparency. No proof exists that the vulnerabilities in electronic voting machines discovered by security researchers over the last decade have been mitigated in anyway. When challenged, the manufacturers, lobbyists, and the media demand proof that these systems are vulnerable. This report details numerous vulnerabilities that may still be present in systems used throughout the country. Because there is no information security infrastructure applications or culture surrounding electronic voting machines, it may be difficult or impossible to detect specific malware or threat actors capable of targeting machines. Instead, it might be easier and more responsible to require voting machine manufacturers to prove to a federal entity that their machines can be trusted beyond a reasonable doubt to ensure the confidentiality, availability, and integrity of voters' cast ballots.

Even if manufacturers released and deployed patches and updates, a large percent of the systems, maintained and operated by State and Local governments would not be patched or updated regularly because most systems are not connected to the internet and because untrained personnel manage most systems. An attacker could infect secured systems with malware by physically mailing an infected USB device with spoofed correspondence and socially engineering an election official into "updating" the machine.

A decade's worth of vulnerabilities leaves a system at severe risk of compromise. Of the systems discussed in this report, at least a third are no longer supported, manufactured, or produced, despite their continued use in United States elections. These systems include, but are not limited to: the iVotronic, the AccuVote OS, the AccuVote OSX, the AccuVote TS, the AccuVote TSX, the AVC Edge, the AVC Advantage, the Optech III-Eagle, and the Optech Insight [1]. Further, some systems, such as the Verity Voting system, the PopulexSlate system, and the ClearVote system, depend on Consumer-Off-The-Shelf (COTS) components that have reached their end of life and are likewise unsupported.

This report enumerates a fraction of the known vulnerabilities in the voting systems used across the United States, including: removable media such as smart cards, ROM modules, USB drives, PCMCIA modules, and flash memory that can be compromised or replaced to infect a system; open internal and external network connections that provide unintended access to a system; unsecured ports that can be used to subvert systems; poorly implemented cryptography and authentication mechanisms; improper source code design; and other vulnerabilities. Nevertheless, this report does not claim to be a conclusive or exhaustive list of the exploitable vulnerabilities in electronic voting machines. Without insight and extensive study of each system, it is impossible to know what vulnerabilities remain undiscovered as of 2016.

Local Level Election Official and Staff Exploitation

Local elections are run by untrained volunteer personnel who lack even the basic understanding of information security necessary to ensure the confidentiality, integrity, and availability of election data. Appendix B contains screenshots of job listings (current at the time of this writing) for local election officers and for election machine technicians at the local level. As shown in the postings, local positions only require little more than a basic high school diploma, possibly a few years of training or experience with technical systems, and the enthusiasm to work on election day. The local level is the prime target for insider threats and adversaries who require physical access to election systems. An attacker could purchase a fake identity on Deep Web for less than $1, and apply for an open position in order to gain access to a machine. Otherwise, they could use social engineering such as spear phishing on local election officials.

Electronic voting machines are often poorly secured in the lowest-bid storage available, such as church basements or minimally secured warehouses. The attacker could pose as an insider, a volunteer, or possibly just walk in as a “repairman” to gain access to a system. Most states minimally test voting machines in the weeks or months prior to an election, but an attacker could easily infect a device after a test or install malware, a logic bomb, or altered physical hardware that does not activate until after the testing period. Local election personnel, devoid of cybersecurity training and awareness, would likely be none the wiser to the attack.

State Level Election Board and Staff Exploitation

Election systems are no more secure at the State level than at the local tier. If an attacker can compromise a central tabulator or breach the main voter database, then they can manipulate voter databases or the results of an election without compromising individual electronic voting machines. Once a cyber adversary compromises one system in the State office, such as a personal computer, a fax machine, or a router, they can laterally move across the internal and external network or they can cross airgaps onto segregated systems using malware that installs itself onto and from any connected removable media. An insider threat, hired for the election season, posing as an employee, or using the stolen credentials of a contractor, can physically manipulate or infect State systems. Remote attacks against State systems can be launched from anywhere in the world, require the least amount of effort, and are the most likely to go unnoticed. Websites belonging to States or frequented by State officials are targeted by SQL injection attacks, man-in-the-middle attacks, and watering-hole attacks. State officials are easy targets for social engineering and phishing campaigns or as unintentional insider threats. Once an attacker has compromised the State IoT microcosm, they can gain access to “Frankensteined” legacy-modern systems, disrupt critical assets, or laterally spread their malware onto every networked device, which in some cases, includes electronic voting machines and central tabulators that communicate with the State system through networked connections.

In May 2016, security analyst David Levin of Vanguard Cybersecurity was arrested (and later released) after he compromised the Lee County, Florida elections website [2]. Levin stated "You could be in Siberia and still perform the attack that I performed on the local supervisor of election website.” He states that an attacker did not need to be in the building where the voter database resided, in the county, or even in the country to trick the system into revealing information or issuing undue access. Levin was able to find and spoof tables and databases, including unencrypted tables of user credentials [3].

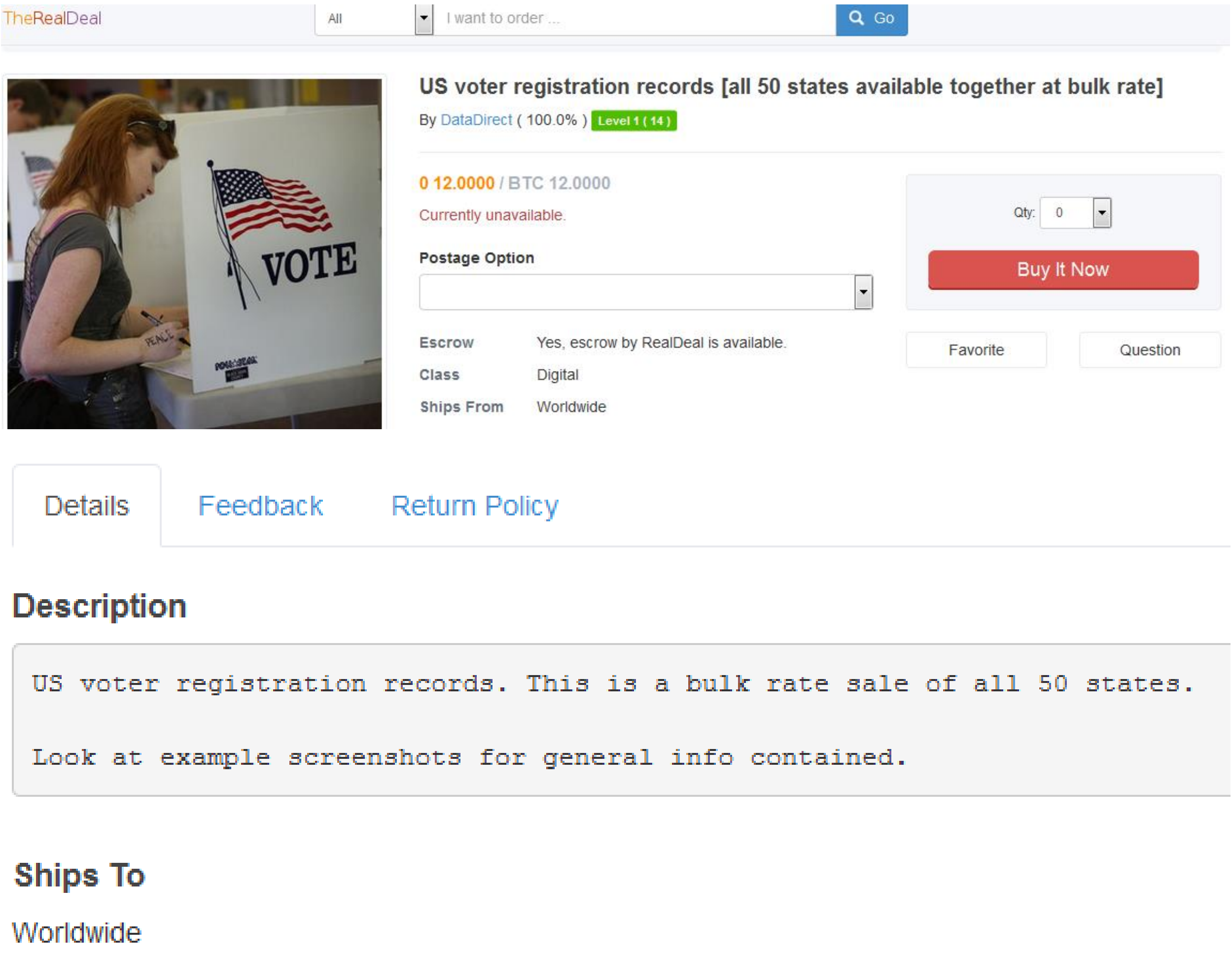
On June 28, 2016, the FBI notified the cyber response team at the Arizona Department of Administration that credentials related to the Voter Registration System had been compromised. Upon investigation, malware was discovered on a County computer, though a causal link was not established [4]. The computer may have been infected by a spear phishing email, a watering hole attack, an insider threat, or through another compromised device. Investigators did not find evidence that data was exfiltrated; however, information may have been improperly accessed or manipulated. The compromised voter registration database contains the name, home address, date of birth, phone number, email address, and party affiliation of the more than 3 million registered voters in the state of Arizona. It also includes the last four digits of each voter's Social Security number, his or her driver's license number and a photograph of his or her signature [5]. The compromise could be an attempt to demonstrate the vulnerabilities in the system, an attempt to steal voter information for identity theft or profit, an attempt to spread fear and doubt prior to November's election, or it could be the precursor of a larger attack.

On July 12, 2016, cyber-attackers launched a campaign against the Illinois State Board of Elections' online voter registration system and caused officials to shut down the site for 10 days. Cyber-attackers breached systems and exfiltrated personal data of up to 200,000 voters. The board's general council is confident that no information in the database was altered [6].

On August 18, 2016, the FBI Cyber Division issued a flash warning that cites evidence that within the last few weeks, foreign cyber adversaries have breached two state election databases. At least one of the incidents resulted in the exfiltration or compromise of voter registration data. The bulletin may refer to the cyber aforementioned intrusions into Arizona and Illinois voter registration systems in June and July 2016, respectively [7]. The FBI told state officials to conduct vulnerability scans of their database systems and to implement the principle of least privilege for database accounts [8].

The two states, likely Arizona and Illinois, are not alone in the vulnerability and compromise of their online systems such as voter registration websites. In fact, during an ICIT investigation of Deep Web marketplaces, a sold out listing was found on TheRealDeal Market offering voter registration record databases from any of the fifty states for 0.5 Bitcoins (~$300), or in bulk for 12 Bitcoins (~$7200).

Figure 1: TheRealDeal DeepWeb Sale of Voter Registration Databases



US voter registration records [all 50 states available together at bulk rate]

By DataDirect (100.0%) Level 1 (14)

0 12.0000 / BTC 12.0000

Currently unavailable.

Postage Option

Escrow	Yes, escrow by RealDeal is available.
Class	Digital
Ships From	Worldwide

Description

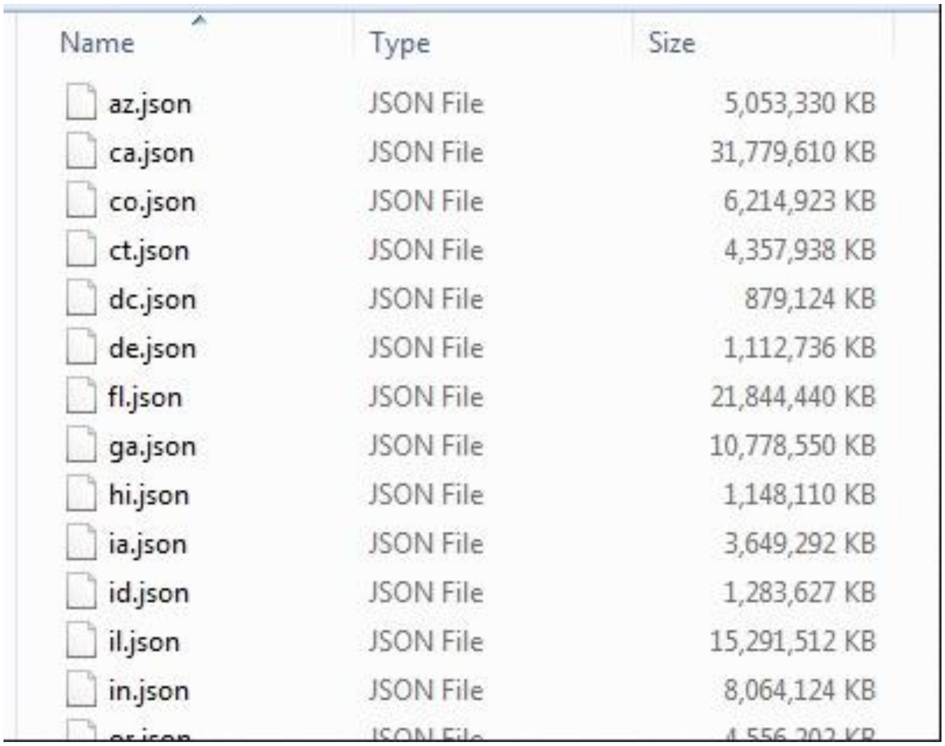
```
US voter registration records. This is a bulk rate sale of all 50 states.

Look at example screenshots for general info contained.
```

Ships To

Worldwide

Figure 1 depicts a sale of bulk voter registration records from every state that were available on TheRealDeal Market of DeepWeb in early September 2016. Individual state databases were available from the same seller for 0.5 Bitcoins each.

Figure 2: TheRealDeal DeepWeb Sale of Voter Registration Sample Files

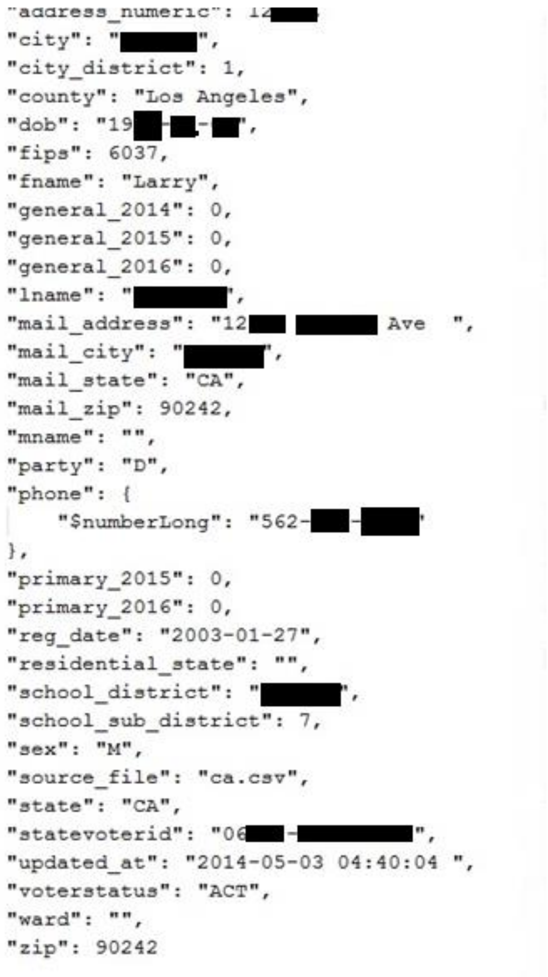


Name	Type	Size
az.json	JSON File	5,053,330 KB
ca.json	JSON File	31,779,610 KB
co.json	JSON File	6,214,923 KB
ct.json	JSON File	4,357,938 KB
dc.json	JSON File	879,124 KB
de.json	JSON File	1,112,736 KB
fl.json	JSON File	21,844,440 KB
ga.json	JSON File	10,778,550 KB
hi.json	JSON File	1,148,110 KB
ia.json	JSON File	3,649,292 KB
id.json	JSON File	1,283,627 KB
il.json	JSON File	15,291,512 KB
in.json	JSON File	8,064,124 KB
or.json	JSON File	4,556,202 KB

Figure 2 shows a sample screenshot of state databases provided by the seller in Figure 1.

Despite the bunk arguments of election officials who lack the technical proficiency to justify claims of system security, state operated election systems are not secure. Simply spear phishing the state election board with application updates or delivering malware/ransomware via drive by download, watering hole attack or malvertising would render virtually guaranteed success by even the most novice of script kiddies. Networked devices are interconnected with non-networked devices. Malware that includes key loggers, RATs, and screenshots would allow any adversary carte blanche access to manipulate and exfiltrate voter registration and election data. Further, systems containing sensitive information continue to be accessible to personnel without information security training. The majority of state voter registration database breaches have not been publicized because election boards are not technically savvy enough to know what to look for or even what questions to ask technologists when it comes to layering network defense to protect voter identities and data.

Figure 3: TheRealDeal DeepWeb Sale of Voter Registration Sample Voter Record



```
"address_numeric": 12[redacted]
"city": "[redacted]",
"city_district": 1,
"county": "Los Angeles",
"dob": "19[redacted]-[redacted]-[redacted]",
"fips": 6037,
"fname": "Larry",
"general_2014": 0,
"general_2015": 0,
"general_2016": 0,
"lname": "[redacted]",
"mail_address": "12[redacted] [redacted] Ave  ",
"mail_city": "[redacted]",
"mail_state": "CA",
"mail_zip": 90242,
"mname": "",
"party": "D",
"phone": {
    "$numberLong": "562-[redacted]-[redacted]"
},
"primary_2015": 0,
"primary_2016": 0,
"reg_date": "2003-01-27",
"residential_state": "",
"school_district": "[redacted]",
"school_sub_district": 7,
"sex": "M",
"source_file": "ca.csv",
"state": "CA",
"statevoterid": "06[redacted]-[redacted]",
"updated_at": "2014-05-03 04:40:04 ",
"voterstatus": "ACT",
"ward": "",
"zip": 90242
```

Figure 3 shows a sample screenshot of a voter registration file from a state database offered for sale in Figure 1.

Despite the Department of Homeland Security's August 15, 2016 offer to help states inspect voting systems for bugs and vulnerabilities, most states, including many of those lacking in Voter Verified Paper Audit Trail (VVPAT), such as Pennsylvania and Georgia, declined the need for federal assistance to secure electronic voting systems [9]. After the 2002 Help America Vote Act (HAVA), most election jurisdictions in the country replaced mechanical and paper punch card systems with either Direct Recording Electronic (DRE) or optical scan paper ballot voting systems. DREs directly record user voting information into memory, oftentimes removable, using input from a touchscreen, dial, or push button. Some DRE systems are paired with a VVPAT printer, which allows voters to visually confirm that their selection matched the cast ballot. VVPATs are only a safety net for assuring that individual machines can be trusted, in isolation. If the VVPAT is networked and compromised or if the ballot records are altered at a later stage, for instance in the central counter, then the VVPAT is less meaningful. The alternative to DRE systems, optical scan machines, count shaded paper ballots at a polling place (precinct count) or at a central location (central count) [10]. Optical ballot scanners can also be compromised, though generally, not all at once.

Larry Norden with the Brennan Center for Justice in New York says, "Today, 80 percent of Americans will vote either on a paper ballot that's read by a scanner, or on an electronic voting machine that has a paper trail that they can review." More importantly, this means that 20 percent of the population, many located in critical states such as Virginia and Pennsylvania, will vote on wholly-electronic systems whose trust and integrity cannot be verified [2]. Despite the obvious problem that a fifth of United States citizens cannot securely cast their votes, this "80-20" split is often touted in the media as a dismissal of the severe cyber-security deficiency in the United States. Over 146 million Americans are currently eligible to vote as of 2016 [11]. Even one percent of votes (1.46 million) are enough to sway an election, let alone twenty times that. This impact is compounded by the detail that many of these voters are in the aforementioned battleground states, such as Pennsylvania and Virginia. Hundreds of votes in a crucial county of a swing state can decide a tight election. Therefore, when up to 29.2 million votes cannot be securely cast, the United States has a severe problem. Further, consider that the remaining 80 percent of "trusted votes" depend on optical scan systems which can be compromised as well, on verifiable paper trails which can be corrupted, and on paper ballots which can be miscounted, falsified, or stolen.

Systems that depend on the audit of verifiable paper trails, on the audits of logs, or on the manual recount of paper ballots are subject to an immense amount of human error and a dependency on the attention and knowledge of the volunteer base. If the verifiable paper trail or auditable paper ballot system is disrupted and officials fail to notice, are the results of an election legitimate? Recounts in most states typically begin with a comparison of the reported result against the central counting system totals. If a candidate still contests the results, the total may be compared against the sum of individual machine totals. Next, ballots may be reprocessed, but are practically never tabulated by hand. If anything, a sample of precincts is selected, recounted, and treated as a representation of the entire population.

The vulnerabilities in election systems expand beyond DRE and optical scan systems. Applications, networked devices, volunteer PCs, and other systems are also vulnerable to exploit. According to Pamela Smith of Verified Voting "If you can get at an election management system, you could potentially alter results, or muddy up the results, or you could even just shed doubt on the outcome because you make it clear that there's been tampering." The vulnerabilities in election systems are a systemic problem that extends beyond the type of system implemented. Many states implemented electronic voting systems with funding provided by HAVA, which ceased in 2006. Many states can no longer afford to replace vulnerable systems. Further, the security on the voting systems is either non-existent or reminiscent of 2006. Under the current system, each state sets specific voting system standards under statute or administrative rule. Some states base their standards on the Voluntary Voting System Guidelines (VVSG) provided by the Election Assistance Commission (EAC) and the National Institute for Standards and Technology (NIST). The VVSG outlines specifications to test voting machines against which address: security, functionality, privacy, usability, and accessibility. The EAC relies on NIST to create technical guidelines and on the Technical Guidelines Development Committee (TGDC) – a group of stakeholders, such as vendors, academics, and election officials – to review the guidelines and make recommendations to the EAC. States that use federal voting system evaluation standards rely on the VVSG, while some others still rely on the predecessor standards developed by the long defunct National Association of State Election Directors (NASED) and the Federal Election Commission (FEC). Thirty-seven states and the District of Columbia use some aspect of the federal testing and certification program developed by NIST, the EAC, the FEC, or NASED, in addition to their state-specific testing and certification [10].

Voting machines must go through a testing process according to state standards and in some cases, federal regulations, after being selected and purchased by local jurisdictions. Vendors are responsible for ensuring that their systems are tested through federally accredited Voting Systems Test Laboratories (VSTL) or other applicable bodies. Nine states require testing to federal standards developed by the FEC, NIST, or the EAC. Sixteen states require testing by a federally accredited laboratory. Twelve states require full federal certification, in statute or rule. Though the FEC certification is not required, the elections director of Alaska may consider whether the FEC has certified a voting machine when considering whether the system shall be approved for use in the state. In California, the Secretary of State adopts testing standards that meet or exceed the federal voluntary standards set by the EAC. Kansas requires compliance with the voting system standards required by HAVA. Finally, in Mississippi DREs are required to comply with the error rate standards established by the FEC, even though no such standards are mentioned and the FEC no longer exists. Nine states and four territories have no federal testing or certification requirements and their statutes and regulations make no reference to standards set by federal agencies, certification programs, or laboratories. Instead, these states rely on state-specific processes to test and approve electronic voting machines [10].

For example, Texas requires voting according to federal standards developed by the FEC, NIST, and the EAC. At the local jurisdiction level, after delivery from a vendor, election officials check that a delivered system is certified by the Secretary of State by verifying the name, model number, and version of firmware / software on the system. The system then undergoes a hardware diagnostic test and a mock election test that measures its logic and accuracy. The former verifies that mechanical components are working correctly and are calibrated. The latter simulates a two-person election and the election custodian checks the results against expected values. Within a 48-hour window, the system is needed for the election and the native operating system, application, or management software is configured. The candidate’s information, precinct information, and other parameters are set. If a test fails, the election custodian prepares a written record of what discrepancy occurred and how to fix the problem. This is a huge opportunity for intentional or unintentional insider threat. After the election, votes are tabulated and sent to a centralized system. Within 72 hours, the election custodian tests the accuracy of the electronic voting system results by manually counting "either all the races in one percent of the precincts or in three precincts, whichever is greater." The general custodian of election records may conduct criminal background checks on election workers prior to hiring. The custodian is responsible for keeping a detailed record of all removable media. The custodian is supposed to ensure that premises are secure and that machines are not physically or remotely accessible. If any discrepancy occurs in the central accumulator system, then the presiding judge of the counting station decides if further audit is needed. The Secretary of State can waive or reinstate any verification requirements [21].

Table 1: United States E-Voting Testing Requirements by State, Territory, and District

Requirements	**Applicable Regions**
Adopts testing standards that meet or exceed the federal voluntary standards set by the EAC	State(s): California
Requires testing according to federal standards developed by the FEC, NIST, or the EAC	State(s): Connecticut, Hawaii, Indiana, Kentucky, Nevada, New York, Tennessee, Texas and Virginia Federal District: D.C.
Requires testing by a federally accredited laboratory	State(s): Alabama, Arkansas, Arizona, Colorado, Illinois, Iowa, Louisiana, Massachusetts, Maryland, Michigan, Minnesota, Missouri, New Mexico, Pennsylvania, Rhode Island, and Wisconsin
Requires full federal certification in statute or rule	States: Delaware, Georgia, Idaho, North Carolina, North Dakota, Ohio, South Carolina, South Dakota, Utah, Washington, West Virginia, and Wyoming
Consider whether the FEC has certified a voting machine when considering whether the system	State(s): Alaska
Requires compliance with the voting system standards required by HAVA	State(s): Kansas
DREs required to comply with the error rate standards established by the FEC (none set)	State(s): Mississippi
Adheres neither to federal testing or certification requirements nor to statutes and regulations that reference standards set by federal agencies, certification programs, or laboratories	State(s): Florida, Maine, Montana, Nebraska, New Hampshire, New Jersey, Oklahoma, Oregon, and Vermont Territories: American Samoa, Guam, Puerto Rico, and the Virgin Islands

One reason that states oppose the federal classification of voting systems as critical infrastructure is because it could mean a federal takeover of a state-run system. Without the knowledge or resources to update the technology, states depend on manufacturers to secure devices. Electronic voting machine manufacturers do not have a reputation for transparency in their design or operation of voting machine technology. Security by design is not common in electronic voting systems and in many cases, security is not even included. These systems will become more interconnected, more accessible, and more vulnerable over time. Without significant change in design, operation, maintenance and oversight, compromise may be inevitable, if it has not already occurred. That said, the security of the election system would likely improve if the systems were designed according to regulatory security standards.

Why Care?

In a representative republic like the United States, individual voters impact the national identity and pervasive culture by casting their ballots either in support of specific decisions or in support of elected officials who are tasked with making decisions in accordance with the needs and opinions of their voter base. The electoral system is the foundational characteristic of American Democracy. Every voter has a minute capability to influence the leadership and laws of the nation through their engagement in the political process in general, and through their vote in particular. Voters trust that their ballots are kept secret, remain secure, and are counted as cast. By relying on non-secure black-box electronic voting systems and complex and all-too-often ignored auditing processes, trust in the systems and integrity of the electoral process cannot be assured. A compromised election could result in loss of faith in American democracy or in the election of a leader who did not earn the position. The likelihood, ease of attack, and direct impact of compromised elections on voters increases at the state and local levels respectively. Safeguards in the American system are meant to ensure that the election of a single candidate, whether through a compromised election or poor judgement of voters, will not tear down democracy as a whole. However, a flawed election can plant seeds of distrust and discord. Imagine the havoc that an attacker could wreak upon the United States by compromising a state voter registration site and using malware or a logic bomb to delete the voter registration of a portion of the population. How much greater would the impact of that simple attack be if the malware only affected the registration of a select demographic of people?

Moreover, an attacker can decide more than just elected officials by compromising e-voting machines; they can influence the ideas upon which society depends. Compromised elections deprive voters of their voice on tax decisions, 2nd amendment rights, social issues, or numerous other decisions. The vote on a controversial social issue, such as LGBTQ rights or England’s Brexit, can have slight margins and drastically different results on society. Polarized issues such as these may incite radicalized lone-wolves, hacktivists, or ideologically opposed nation states to interfere with the American democratic process by manipulating the voting systems that store, tabulate, and determine the vote.

Vulnerable electronic voting machines have been in use for over a decade in some parts of the United States, and there is no conclusive proof that attacks have not already occurred. The threat posed by relying on vulnerable electronic voting systems will increase as the pervasiveness and ubiquity of the internet increases in proportion to the age and vulnerability of the systems.

Voting Systems by Manufacturer

This report demonstrates some of the vulnerabilities discovered in notable electronic voting systems and applications. A robust table of manufacturers, models, types, and regions where the devices are used in 2016, can be found in Appendix C. For the sake of brevity, only a selection of the systems included on Table 1 is discussed below. The information provided in this report is based on the research of security professionals and on publicly disclosed vulnerabilities. Due to a lack of transparency in the sector, it is difficult to say if any of the vulnerabilities described have been patched or mitigated since their discovery; however, given the decentralized and disorganized state of the sector, it is likely that unpatched, vulnerable systems remain in operation, even if the manufacturer or state has done their due diligence.

Avante

Vote-Trakker

The Avante Vote-Trakker is a DRE with touchscreen that can be equipped with a VVPAT printer. The reported problems with the Vote-Trakker system mostly amount to problems with the paper audit trail, and it demonstrates that despite popular discussion, DREs are not the only poorly designed e-voting systems. The printer reel requires replacement after every 600 votes. A VVPRS indicator light informs the user when paper is low, but the warning can be dismissed. If the voter continues, there is a chance that their vote will not be recorded on the audit trail. Election officials are not notified when any problem occurs with the VVPRS. Further, the paper record does not distinguish between accepted or non-accepted ballots. The name of the election is not included on the printed record. It may be possible to slip unauthorized or forged ballots into the ballot storage area through a slit between the printer and the ballot storage unit [13].

Advanced Voting Solutions (AVS)

WINVote

WINVote is a now defunct system that exemplifies how vulnerable e-voting systems can be and why the systems should not be networked. It is a DRE-touchscreen system equipped with a wireless local area network (LAN) connection, modem, and printer. The system uses 802.11b wireless technology to open voting machines to program ballots. Ballots are then transmitted via wireless networking. The system uses the WINware software for election management and the WINprep software to allow county officials to perform all aspects of the election programming process. The WINresults software is used for tabulation, accumulation, and reporting. In some areas, poll workers were required to manually transport the entire WINVote systems to the tabulation facility for tabulation, but in some regions, workers were allowed to remove and transport the internal USB flash drive. Data including hardware, diagnostic test logs, ballot images, ballot cast logs, operational audit logs, ballot images, and use activity from the polling location are collected and stored in single USB type memory devices for archive and audit use [12].

During the 2014 election, a Virginia precinct reported anomalous activity on a WINVote system. The Virginia Information Technologies Agency (VITA) was asked to perform a security analysis of the devices. VITA used known exploit techniques and open source platforms to realistically compromise the WINVote systems. VITA was not provided with any information about the existing security controls or security posture of the black-box proprietary system.

Security deficiencies were identified in five key areas, such as physical controls, network access, operating system controls, data protection, and the voting tally process. Physical security on the device amounted to an easy to bypass lock that allowed access to a USB port. In proof of concept of an attack, VITA accessed a port and used it to access a machine’s BIOS and modify its boot order. They altered the machine to boot a different operating system, Knopix, and take images of the system drives. While compromising a machine in this way might be noticeable in public due to time and the location of the USB port on the top of the system, it can be discretely done in isolation by an insider threat or with a smaller, less noticeable boot device. WINVote machines can be attacked from a remote location through the 802.11b wireless protocol. Each device was set to a default peer-to-peer configuration with WEP encryption. The devices even broadcast their SSIDs. While each device has the ability to disable the wireless network from within the application, it does not disable the network interface. Disabling the interface just makes the application no longer seek other networked devices. Because the network card remains active, it can still send and receive traffic. VITA found that it was not possible to disable the network connection using the WINVote application. Researchers attempted to mitigate the vulnerability, but they found that either the physical removal of the wireless adapter or changes to the device software rendered the WINVote device unable to administer an election. The testers were able to crack the WEP key (“abcde”) and join to the WINVote ad-hoc network in less than two minutes. Once on the network, VITA used Nmap and Nessus scans to search for recognizable vulnerabilities. The system had no firewall and TCP ports 135,139, 445, 6000, and 1601 were open. The Nessus scans also uncovered eight critical, three high, five medium, and two low-risk vulnerabilities.

The Windows XP Embedded 2002 operating the WINVote system had neither patches nor service packs applied. Consequently, the operating system was vulnerable to over a decade’s worth of vulnerabilities. The testers targeted the file sharing service and file shares with Nmap and Nessus and they performed a brute force password attack using the open source tool Hydra, and a standard wordlist. They found that the “Administrator” account password was set to “admin”. The credentials could be used to RDP into the system or to map network shares to identify vulnerabilities that would allow remote modification of the device. The attack succeeded without any level of sophistication, though many of the individual exploits failed because the target system was too old for them to run.

VITA researchers targeted the unencrypted Microsoft Access database that stores ballot information and the results. The password "shoup", used for all database files, was discovered in approximately ten seconds. With the password, researchers could copy the database files to the security analysis system, open the files and modify the voting data. The altered files remained on the system when the system files were replaced. By modifying the database, the researchers were able to alter the election tallies. Ultimately, the security audit found weak security controls, insecure and insufficient encryption protocols, weak passwords, and insufficient system hardening. Passwords were less than seven characters and did not follow any best practices. Passwords were weak and standardized across machines. Wireless traffic was intercepted in less than two minutes, and the weak WEP communications key was rapidly compromised using open source tools. The voting device was not hardened with security in mind. Patches, service packs, and basic perimeter and endpoint security were all absent. Finally, the databases containing voting data were not encrypted, could be modified without knowledge of the password, could be accessed by cracking the weak password, and access to the database enabled the ability to modify election results. VITA concluded that the systems were so insecure that WINVote systems should not remain in service [14].

Clear Ballot Group

ClearVote

ClearVote is a newer system with more secure systems and more transparent design and operation. It is a paper-based voting system that includes the ClearCount P1000 precinct optical scanner, the ClearAccess touchscreen, and the ClearCount central count scanner which depends on an unmodified COTS printer, such as the Fukitsu fi-6800. The ClearAccess software records voter choices and prints machine-readable ballots that are scanned and tabulated in the same stream as voter-marked ballots [12]. The primary vulnerability of the ClearVote system is that it depends on COTS systems. The manufacturer cannot assure the integrity of the underlying components, which could be infected with malware or left otherwise vulnerable prior to their inclusion in the device. On the other hand, reliance on COTS components increases transparency and ease of maintenance.

ClearAccess is designed to run on COTS computers that run Microsoft Windows. Newer machines reportedly run on a hardened Windows 8.1 operating system. The ClearAccess file system consists of four files. Config.txt contains machine configuration information. State.txt contains information about the currently loaded election and in what state it occurs. System.log records all non-election specific activity and it appends the log whenever users log in or log out, fail to log in, or when any other change is made to the system. Finally, election.log is created when the election is loaded and its records are appended whenever there is any election-related activity. ClearAccess depends on role-based access and permission controls. The role of the user determines the data elements that the system has access to and the actions that can be performed on those elements. Voter accounts can only access a ballot. ClearAccess checks the permissions and all operations are based on the permissions granted to the role of the current user. It thereby prevents a restricted user from being able to access or modify anything that is not explicitly permitted by their own permissions. The access controls for the ClearAccess system requires explicit permissions to access any operation, privileged or other. Valid user credentials and passwords are required to upgrade or install software. Poll worker accounts can open and close polls and can view the logs. Maintenance accounts can access system setup and logs only to help diagnose any issues. The account cannot access election data. An Administrator account can access system setup, logs, and load and unload elections, but they cannot access election data. Finally, the Election Administrator can access election data, view the logs, do pre-election testing, and prepare the system for voting. ClearVote minimizes its attack surface by excluding any communication networks such as telecommunication and public or wireless networks [15].

Dominion Voting Systems

ImageCast Democracy Suite

ImageCast is a prime example of a vulnerable optical scan system and its associated components. It debunks the notion that only DRE systems are vulnerable to malicious adversaries. The Democracy Suite is a paper-based optical scan system that includes an Election Management System (EMS), the ImageCast Precinct (ICP), a precinct-based optical scan ballot tabulator, the ImageCast Evolution (ICE), a precinct scanner with optional ballot marking capabilities, and the ImageCast Central (ICC), a high-speed central ballot scan tabulator based on COTS hardware. As with ClearVote, the use of COTS components increases transparency, but it may also increase the attack surface. The ICP has a small touchscreen to allow users, ranging from poll-workers to attackers, to access diagnostic and configuration settings. The system scans and interprets voter ballots and stores and tabulates each vote from each paper ballot in compatible ballot storage boxes. An ATI device provides additional accessibility to voters through “sip and puff” or by allowing them to listen to options as audio with variable speed and playback functionality. Because the ATI is directly connected to the tabulator, there is no paper ballot when votes are cast using ATI; further, the direct connection can be exploited by an attacker to gain control over the system. The ICE scans, interprets, and tabulates voter ballots and it displays them back to the voter through an LCD display. The ICC is a central ballot tabulator that relies on a Canon DR-X10C or Canon DR-7550C scanner and a proprietary ballot processing application software [12]. Exploits for these COTS systems can be easily found online and used to disrupt the paper audit trail.

In one 2012 Wyle Laboratories security assessment of the suite for the EAC, the EMS, which was hosted on a Sell Precision T1500 with a Rocsecure Commander 2UE external hard drive, password policy complexity was disabled, administrative and guest accounts had not been disabled or renamed, the backup and restore privilege was disabled, “audit shutdown system if unable to log security audits” was disabled, “FIPS Compliant Algorithms for Encryption Hashing and Signing” were disabled, and several user accounts were found to perform tasks outside their defined roles. Analysis of the ICP found that USB ports were properly disabled and the RJ45 connector only allowed for operation of the ATI device. Networked connection to the system was disabled (except the connection light) and no information was accessible. In the ICE, a hole was discovered in the ballot box that was large enough to permit “ballot stuffing”. All other access points appeared to be locked or sealed [17].

Election Systems and Software (ES&S)

DS200

The DS200 is a vulnerable precinct-based optical scan system consisting of a voter-activated paper ballot counter and vote tabulator with an LCD touchscreen and a printer. Votes are stored on an internal memory card. Optional landline and wireless modem connections are available for the units. These network connections can be leveraged to gain access to the device. The DS200 also captures digitized images of all ballots scanned for the purpose of write-in or unclear ballots. At the polls close, DS200 prints out the voter logs so election officials can tally votes. All ballot data is stored on a removable USB flash device. The USB drive is secured via a weak physical lock compartment. According to Verified Voting, “The DS200 source code consists of C/C++ components with a modified ESSUNITY3200 baseline that was modified during the Unity 3.2.1.0 EAC test effort. In total, 651 functions were changed and were reviewed by the EAC for conformance to the VVSG 2005. 42 instances of non-conformance were reported to ES&S, which submitted fixes and validated issue resolution. All source code discrepancies were comment related and were not against any of the software related VVSG 2005 requirements. The file function line count results identified no files or functions exceeded 240 eLOCs, 3.47% were between 60 and 120 lines, .23% were between 120 and 240 lines, the remaining 96.30% were less than 60 lines”.

Attackers may be able to additionally affect the DS2000 by ripping the corners of ballots and causing an anomaly, attributed to Unity 3.2.1.0. In discussion with the EAC, ES&S stated that they have only been able to replicate this issue in testing by removing the plastic guides and physically altering the ballot (cutting of a corner). In the course of the review, the EAC found various degrees of ballot image distortion, with the 17” ballot having the largest degree of skew. Further, the EAC found that if an election definition contains more than 40 ballot styles, the user has to define more than one absentee precinct and then separate the ballots into groups for processing. In addition, all optical scan ballots used in a given election must be the same size and have the same position capacity. An early vote station will only support a maximum limit of 9999 precincts meaning that a large number of precincts may result in small ballot processing delays, and an early vote station will not be able to print a precinct-by-precinct report by default [12].

InkaVote

The InkaVote and InkaVote Plus system consists of the InkaVote Precinct Ballot Counter (PBC), based on a standalone lottery ticket machine, and the Unisyn Election Management System (EMS). The InkaVote ballot is based on the design of a Hollerith (IBM) punch card, with ballot identification data pre-punched in the leading columns. The InkaVote Plus PBC unit may be equipped with an optional component called the Audio Ballot unit, which provides support to assist the visually blind as well as other voters who need an audio ballot. The Audio Ballot unit consists of a keypad, earphones and printer. As in aforementioned systems, the support system can be leveraged to gain control of the system.

The InkaVotePlus has numerous unresolved vulnerabilities, including inappropriate use of symmetric cryptography for authenticity checking, reliance on a weak home-brewed encryption algorithm, and weak cryptographic key generation based on weak entropy which is susceptible to brute force attacks. The code and comments indicated use of a checksum method that is suitable only for detecting accidental corruption and is used inappropriately with the claimed intent of detecting malicious tampering. Approximately 106 SQL statements were embedded in the code, with no evidence of sanitation of data before it is added to the SQL statement. Physically, the tamper-evident seals were easily removed intact using household chemicals and a razor blade. The lock was able to be picked with office supplies. The USB port can be used to deliver malware or gain control of the system. An attacker can attach a standard keyboard to the keyboard connector for the Audio ballot unit. Finally, the PBC head was able to be removed (to insert or remove ballots) without breaking the seals [12].

iVotronic

The iVotronic is a DRE-touchscreen system that is made vulnerable by its voter authentication token, the Personal Electronic Ballot (PEB). A PEB is a media that can be deactivated and reassigned by poll-workers in order to be used in multiple iVotronic machines throughout the day, provided that they are used in the same election at the same polling place. PEBs are programmed at a supervisor terminal at the start of an election and are also used to store ballot definitions and election results. PEBs can be read using a supervisor terminal or with a dedicated PEB reader connected to a machine running the Electron Reporting Manager application. Poll-workers connect PEBs to machines after voter authentication. The PEB communicates with the machine via infrared signals. The PEB only allows a voter to cast a single ballot. Voters place their votes on the touchscreens. Some voter iVotronics store large ballots, audio ballots, and election audit files on compact flash cards. Votes are recorded to three internal flash memories and a fourth, removable compact flash card, similar to a digital camera card. All of these cards can be corrupted or removed. An independent Communication Pack is connected to iVotronic terminals at the start and end of elections to print zero count tallies and precinct results on an independent printer. At the conclusion of polls, the summary data from each machine is loaded onto a PEB using a supervisor password and then the PEBs, compact flash cards, and any printouts are either physically transported to election headquarters for aggregation or their contents are transmitted over a computer network using a laptop running ES&S Unity Software.

Ohio, West Virginia, and North Carolina require the Real-Time-Audit-Log (RTAL) by law, but the option is not available in South Carolina, Texas, and Pennsylvania. The RTAL printer is a reel-to-reel printer under transparent plastic at the left of the touchscreen. RTAL records all voter actions, even if they change their mind. This provides an immediate effect back to the voter, though it can also complicate the auditing process. It also denies voters the option to review all of their options at once prior to submission [12].

The PEB slot on the front of machines is particularly vulnerable. An attacker can gain privileged access to the system using a magnet and a properly programmed device with an infrared port (such as some phones, PDAs, or remotes). An attacker who gains access to a PEB for an extended period of time can change votes or load malware to attack the central Election Management System when the PEB is returned to election headquarters. An attacker could also disconnect the VVPAT printer by unplugging the cable at the top of the machine [12]. iVotronic version 8 and version 9 had three character passwords for some systems. A hardcoded key was used to obfuscate passwords before storing them in a database. The algorithm used to encode the data was weak and reversible. An attacker with access to the scrambled password could easily decode the actual password. This vulnerability may be the result of the implementation of weak homebrewed encryption algorithms [18].

Model 100

The majority of electronic voting systems do not encrypt data where it is stored, processed, or in transit. Consequently, most machines can be attacked by physically removing or compromising their removable storage media. The Model 100 is an example of such as system.

The Model 100 is a precinct-based optical scan system consisting of a voter-activated paper ballot counter and vote tabulator that uses visible light scanning to count and record voter information from paper ballots. The unit depends on an Intel 80386 microprocessor to process data from the image sensor and an internally stored PCMCIA memory card to record election results [12]. A 2007 red team analysis of the Model 100 by Freeman Craft McGregor Group for the State of California found that PCMCIA cards could be easily swapped and that the attack would likely remain undetected. The data on the PCMCIA cards was not encrypted and data could be manipulated. Analysis of the source code found that the documented structure of the information stored on the PCMCIA chip did not correspond to the implemented structure. The back-end Election Reporting Manager (ERM) has an exploitable built-in feature to add or remove votes from the vote tallies, though use of the feature is recorded in the audit logs. The ERM relies on a password constructed from publicly available data, which is listed in the documentation, and cannot be changed [18]. Compounded with the previously discussed feature of the ERM, anyone with access to the ERM documentation can access the ERM and use a built in feature to alter vote tallies.

Analysis of the source code found that the M100 ballot counter was designed to load and dynamically execute binary files that are stored on the PCMCIA card containing the election definition files in clear text without effective integrity protection. Therefore, the election officials can never trust the results from the electronic vote tabulation without confirming the results with a statistically significant random sample of corresponding paper ballots [18].

Hart Intercivic

Ballot Now

Ballot Now is Hart's software for on-demand printing of paper ballots and scanning and resolving batches of ballots. Ballot Now is mostly used to tabulate absentee ballots. The system relies on Hart's EMS software suite, a Windows 2000 Professional machine, and one of a variety of third-party scanners, such as the Fujitsu M4099D or the Kodak i830. Ballot Now can be operated as a standalone machine or it can be networked in a client/ server configuration if the user configures the proper network certificates. If run in standalone configuration, the eCM must be present on the machine, if ran in a networked configuration, the eCM must be present on the Ballot Now server. The system is vulnerable if networked. It is likewise susceptible to exploits against vulnerabilities in its COTS components, exploits of unpatched vulnerabilities in Windows 2000, and to attacks against its certificates.

In a report prepared by teams from Pennsylvania State University, the University of Pennsylvania, and WebWise Security, Inc. as part of an EVEREST voting systems analysis project initiated by the Secretary of State of Ohio in late 2007, researchers found severe vulnerabilities in Hart systems, including the Ballot Now system. Hart systems failed to protect the integrity of election data because virtually every ballot, vote or result could be forged or manipulated. Systems were plagued with numerous undocumented features that allowed for remote script attacks in which votes could be spoofed or repeatedly counted. Malicious insiders could access systems because access controls such as physical security, passwords, and cryptographic keys were easy to circumvent. The auditing capabilities of the systems were limited and were vulnerable to a broad range of attacks. Due to the lack of transparency and an abundance of undocumented features and services, the full functionality and exposure of Hart systems remains unknown. The burden of security was entirely placed on preventing physical access to systems. When physical security policies were not followed or were not defined, attacks were difficult to preempt, prevent, or identify [19].

The researchers also discovered that the "Autovote" feature included in the Ballot Now back-end server application allows users to print eScan ballots whose votes are pre-cast, in bulk. The feature is likely a test apparatus used to mimic election conditions. Autovote is not available by default and is only accessible when a combination of registry entries are set to specific values. Each ballot has the word "AUTOVOTE" printed on the side and is only accepted when the ballots are fed into an eScan in test mode. It may be possible to change the printed "Autovote" banner to any text, including no text. Autovote is not mentioned in product manuals or technical documentation, save for a brief mention in a 2001 manual (which was later removed) and several mentions in e-voting hearings from 2001 and 2003. When other specific registry values are set, Autovote ballots can be accepted in the "election" mode, which is used for live elections. If the entry is set when Ballot Now is used to process ballots with a high-speed scanner, then the Autovote ballots are accepted as legitimate. An internal or external adversary with access to the Ballot Now server and a precinct scanner can thereby spoof votes to impact the election tally [19].

eScan and eScan AT

The eScan is a precinct optical scan system that stores voter ballot images as a Cast Vote Record (CVR) on a flash memory card that is removed and tabulated at the close of polls. The eScan is a dedicated proprietary piece of hardware with a built-in automatic feed scanner, a thermal line printer, local flash memory, and two secure compartments for ballot storage. It is intended to only be used with ballots that are printed in advance on paper of a specified weight and dimension. Voters and poll-workers feed paper ballots in one-at-a-time and the unit captures a digital image and separates the ballots into bins [12]. The eScan system is managed by an accessible Ethernet port, located at the back of the machine, which an attacker could access to perform management operations such as modifying the configuration file or reading system memory. Security researchers have also found that some eScan systems, which use Microsoft Windows CE, run a telnet service that makes the machine function as a telnet server. The purpose of the service is unknown, but an unsophisticated threat actor can use the server to subvert the eScan system [19].

EScan configuration options are defined in the Ballot Origination Software System (BOSS) when the election is defined. The units are configured by SERVO, which resets the time, public counter, CVRs, signing key, and audit log. The units maintain audit logs that include system startup and shutdown information, CVRs written and other events like ballot rejection overrides. SERVO also optionally resets MBBs in the eScan to clear the CVRs and audit logs. SERVO can also back up CVRs and audit logs from the eScan, and create a Recovery MBB from those records. The eScan A/T incorporates an audio tactile interface (ATI) to enable disabled voters to listen for instructions and cast ballots [12]. The eScan MBB is unencrypted and it contains access codes that can be used to enable administrator operations such as opening and closing polls on the eScan and JBC [19].

In 2007, the California Secretary of State conducted a red team penetration of Hart systems and found some damning results. The networked interfaces in Hart systems are not secured against direct cyber-attack. Poll-workers and attackers alike can connect to the JBCs or eScans over the management interfaces and modify device functions and software. The threat actor could subvert machines and directly manipulate election results. The insecure functionality is not an unintentional vulnerability, rather it was poorly designed with convenience as a greater priority over security. Further, the Hart software fails to check the validity of input from other units and it uses these inputs in unsafe ways.

For example, SERVO, which is used to back up and verify the integrity of polling place devices, can be compromised from infected devices [20]. SERVO is also susceptible to buffer overflow attacks that would allow an adversary to execute arbitrary code. One use of SERVO is to verify the integrity of the firmware on a JBC, eSlate or eScan by comparing the SHA-1 hash of that device's firmware image to a hash supplied by Hart. Non-matching hashes result in an error. However, since SERVO depends on the device to provide its own firmware image, a compromised device can simply store an uncompromised copy of the firmware image, and provide it to SERVO as prompted [19].

An attacker could subvert a single polling device to subvert SERVO, and then use SERVO to reprogram every polling place device in the county. The systems lack cryptographic security protocols to secure the communications between devices. Consequently, devices communicate in clear text. Hart did employ cryptography for MBBs, but they naively relied on a single, country-wide symmetric key that effectively allows an attacker to forge ballot information and election results. The weak key is stored inside vulnerable polling devices and an attacker can compromise a single device, and then forge election MBBS to disrupt or sway other devices or the result. Finally, Hart's systems fail to protect the confidentiality of voter ballots because a poll-worker could identify an individual voter by reconstructing the order that voters cast their ballots [20].

A 2007 follow up study for the State of Ohio found that obtaining the county key to an eScan system was trivial because with only a few seconds of physical access to precinct or back-end equipment, an attacker could download the key from the eCM manager into a file or extract the key from an eScan's memory via the unprotected Ethernet port. An attacker can forge keys to authenticate to Hart applications such as Tally, BOSS, Ballot Now, eCM Manager, and SERVO because the tokens can be created by anyone with access to a county key. Further, armed with the county key, the attacker can forge any election data they want because the modification would only be detected by careful comparison with the relevant VVPATs or physical ballots. Since the VVPAT is also forgeable, reliance on that countermeasure is only of limited use. If both the MBB and VVPAT/completed ballots are forged, then there will be no way of detecting the forgery short of studying the internal audit information in each eScan and JBC used. Since that audit information can be erased by an attacker with physical access to the device, an adversary can perpetrate undetectable precinct-level forgery of an election [19].

Audit data is protected on the back-end EMS servers in databases that may or may not be encrypted. The passwords for the EMS databases are available in the easily decrypted security databases and can be easily bypassed. With database access, an attacker can also manipulate election results and audit data [19].

eSlate

The Hart Intercivic eSlate is a DRE-Dial system in which a voter selects their ballot options using a selection wheel and five buttons. The system is directly connected to the Judge's Booth Controller (JBC) via a cable that daisy-chains eSlate units together. The JBC provides machine activation and ballot storage for up to twelve eSlate machines. Poll-workers issue voters randomly generated four-digit Access Codes from the JBC, which voters use to access eSlate machines. Results are stored in redundant and physically separated locations on the eSlate internal memory, MBB flash memory, and JBC internal memory. The ballots are transmitted to the JBC via a cable and are stored on an MBB flash memory card, which is physically transported to the election headquarters for tabulation at the conclusion of the election. The eSlate can be adapted to run in disabled access unit (DAU) mode, an accessible mode that offers the same functionality, but is dependent on different hardware inputs and a PCMCIA card to locally store ballot information for audio input, sip-and-puff input, or jelly switches.

The Verifiably Ballot Option printer is a reel-to-reel cash-register style printer that is located to the left of the screen. The printer prints a human readable and a machine readable print out of voter selection options that is spooled out of sight after the voter has confirmed their ballot, to prevent the next voter from seeing the previous voter's ballot. After a maximum number of permitted ballot reviews or cancellations, the system forces the last ballot and VVPAT to be recorded. The machine code is a two-dimensional barcode that encodes the contents of the VVPAT and basic information about the election in which the vote was cast and the machine on which the ballot was cast. The machine can be configured with a Ballot Key serial number to detect duplicate ballots [12].

One of the primary security flaws in the eSlate system is the cable that daisy chains systems together and the cable which connects to the JBC [12]. Commands through the JBC serial connection are not verified; therefore, an attacker can connect to the JBC port and control the eSlate machine as the JBC would. The JBC is managed by the SERVO application through a parallel port (labeled "printer) in the back of the unit. Anyone can access this port to gain control over the JBC and any connected eSlates. Similarly, the JBC has an accessible DB-9 modem interface at its back, in which a serial Voter Registration Interface (VRI) is connected. The VRI can send instructions to the JBC to generate voter access codes for use on the eSlate machines [19]. The eSlate, like many other systems relies on voter codes to authenticate users. The JBC generates the first voter code at random and then it follows a simple mathematical function to generate subsequent codes. Any threat who knows any voter code can therefore determine all other voter codes in the order that they are assigned [19]. Consequently, the codes could be used to cast multiple votes or to alter voter records.

The typical communication between the eSlate and the JBC includes system management, ballot and CVR transfer, and the validation of voter access codes. Because neither the connection nor the data transfer are authenticated or encrypted, a threat actor can use a man-in-the-middle attack or other vector to eavesdrop or intercept traffic between the machines. On the other side, the JBC does not verify that the eSlate system only provides one vote per voter code. The check to see that a voter code is correctly processed is on the eSlate; hence, a compromised eSlate can ignore the checks and issue false votes. While both the eSlate and the JBC check the integrity of blocks of used internal memory every 10 seconds, the checks are trivially bypassable and are very unlikely to detect a system compromise [19]. The JBC verifies the integrity of attached eSlates through a CRC check against the eSlate and its version number; however, if the eSlate is compromised, then it does not have to respond honestly to the JBC's request for information [19].

The last eSlate in the line of connected machines is particularly vulnerable because it has an empty serial cable port on top (which would otherwise feed into the next machine in the line). A malicious adversary can exploit the port by connecting their own cable or device to gain unfettered access to the software in the eSlate and JBC as well as vote data stored locally on each eSlate and remotely on the JBC. To mitigate the risk, the last exposed serial port will be covered with a security seal or otherwise disabled. While a seal or covering might prevent exploitation during an election, they do not prevent an insider threat from accessing the eSlate machine during storage. The JBC and the JBC ports are similarly vulnerable to attack. If a JBC is compromised, an attacker can allow duplicate voting by printing multiple access codes, they can cast votes, they can erase votes, and they can otherwise alter results. Compromised MBB flash cards in the JBC can be used to introduce malware, to cause the election server to crash, or to alter results.

The VVPAT system can be interrupted or disrupted by jostling the unit. It can also be jammed or made to jam. The entire unit should be replaced when a jam or error occurs [12]. Further, the VBO record is printed by a device, the VVPAT, that is under the control of an attached program, eSlate, which could be compromised. As such, the use of the VVPAT could be prevented or perverted to invalidate legitimate votes or to insert illegitimate votes. Alternatively, the VBO interface allows the controlling software to instruct the VVPAT to rewind the paper reel. As such, it may be possible to overwrite legitimate ballots using a compromised system and the VBO software.

When poll-workers close the polls, they have the option of generating three different reports on the eSlate machines: a voter code summary report, a vote tally report, and a write-in report. The write-in report does not perform input filtering on entered data, meaning that it is possible to enter code instead of text. Entering code on the JBC allows user entries to be interpreted as *printf* format strings, which allow the user to possibly execute code or to extract code from the stack or heap and print data on the reports [19].

Populex

PopulexSlate

The PopulexSlate can simultaneously act as a Judge station, a Ballot Counting station, a Voting station, and a Personal Verification station. This provides redundancy in that a failed PopulexSlate system can be replaced with any other PopulexSlate system; however, this increased functionality also poses a significant security risk. The PopulexSlate includes a smart card reader that can authenticate users or program the system, a printer slot for blank ballots, a touch-screen interface for user input, a special stylus (the machine does not respond to touch or other objects), a standard numeric keypad for password entry and ballot navigation, and a hand-held barcode scanner. The internal components and software are all COTS products such as a Lexmark Z605/ Z615 inkjet printer and a Compaq TC1100 tablet PC. Though enclosed in the Populex casing and held in place by Velcro, the latter has a 20MB removable hard drive and USB, infrared, and Ethernet ports. The TC1100 also contains a built-in wireless network interface, though Populex claims that these interfaces are disabled. The TC1100 operates on a version of Microsoft Windows XP Tablet PC edition. Populex's Polling Place Functions (PPF) application software runs as a shell if the user logs into the OS using the standard operator password. The shell is restrictive and confines the user to the PFF application, unless the user restarts the TC1100 unit and enters an administrative password. The administrator has full access to the TC1100 PC, including full read/write hard drive access, permission to install and run executable files, full access to Windows Access Control (including the ability to modify or reset passwords) and Administrative access to enable, disable, or modify OS services.

The TC1100 is contained in a molded plastic housing that is secured by a small metal tab on the chassis that fits into a housing in the cover. There is no built-in physical lock, but a small luggage lock or tamper-evident seal can be placed through the tab. The unit has no service hatches. The cover must be fully opened for any maintenance task.

The manual visual ballot verification process is complex because ballot options are printed as punch numbers that must be translated back to the voter selection using another printout. As originally designed, nothing prevents a voter or poll-worker from registering multiple ballots because the system requires voters to scan their final ballots beneath a barcode scanner prior to dropping it into a ballot box. An attacker could scan the code multiple times before dropping the ballot. The only control is an audit of the results, which may not be done if not required by the state or if suspicions are not aroused [12].

Premier / Diebold

AccuVote

As demonstrated in the 2006 "Hacking Democracy" documentary and as discussed in Part 1 of this report, the AccuVote systems produced by Diebold are notoriously insecure. The systems feature almost no security and are susceptible to internal software bugs and external attacks.

The AccuVote OS is a precinct and central accumulation optical scan voting system that integrates the vote tabulation and recording process into one unit. The system is used in approximately 900 jurisdictions as of 2016. The AccuVote OS system is secured with a physical lock that shares a key with every other AccuVote OS system [12]. The lock can be easily picked or broken to gain access to the internal components of the machine. Each system has one or more ballot boxes that can be filled with fake votes at the start of voting and can easily go unnoticed. The memory cards used in the systems can be corrupted to introduce malware, to cause the election server to crash, or to alter the results of an election.

The AccuVote OS Central Count Scanner is the same as the AccuVote OS detailed above except it has a different firmware installed, that designates it as "central count" instead of "precinct count". Its configuration allows it to be networked with other AccuVote OS units so that voting data can be concurrently sent to the GEMS server. The unit is often used to count absentee, provisional, and damaged ballots. Unlike the precinct version detailed above, the central count scanner is practically controlled by GEMS. The unit does not tabulate or record ballot records. Consequently, the internal memory card does not contain ballot definitions; instead, it only contains some technical information and data to trace ballots back to the individual machine [12]. An attacker would be most interested in compromising the system through GEMS to alter the reported tallies or through accessible memory or drives to gain access to GEMS.

The AccuVote OSX is a precinct and central accumulation digital scan voting system that integrates the vote tabulation and recording process into one unit. The OSX is a high-resolution image-based optical scanner and ballot box. It comes installed with AccuVote OSX software that runs on top of a Windows CE OS. Election and ballot information are defined in the GEMS application and downloaded to PCMCIA memory cards. The system communicates with GEMS over a local area network, a modem, or a direct connection to allow an administrator to select options on a secured and covered 3.5” LCD display to perform pre-election and post-election operations. Access to the system is controlled by smart cards and passwords and it supports user defined keys. The system produces logs, reports, and status messages on a thermal printer, generates audit log records for every transaction performed on the unit while it is powered on, and protects access to: the printer and memory card compartments, the rear power button, the smart card reader, and communication connections. Ballots are processed in the polling place and are not transported to a central location. Each ballot is only touched by the voter between the time that it is cast and the time that it is counted. The unit is powered by an internal and an external battery. The AccuVote OSX had issues with its hardware Protective System Counter (PSC) in the past where the system counter was only resetting to zero during graceful shutdowns. The issue is supposedly fixed by archiving the previous count after each cast ballot [12]. An adversary can manipulate the counter by forcing cyber or kinetic manual shutdowns or by corrupting the archived counter. If the memory cards used in the systems can be corrupted with malware, then the counter can be corrupted or the attacker could introduce malware to periodically shut down the system.

The TS and TSX are DRE-touchscreen systems that are accessed through voter smart cards and that record votes on internal flash memory. The machines are configured through a memory card that is inserted into a slot that rests behind a locked component hatch on the side of the machine. The card stores election definition files, sound files, translations for other languages, interpreted code that is used to print reports, and other configuration information. Voters authenticate to the machine with smart cards that are activated by poll-workers. After voting, the smart card is returned and reactivated for the next voter. Supervisor smart cards are used to authenticate poll-workers and to provide additional functionality, such as the ability to close the polls, put the machines in post-election mode or examine audit logs. Ballots are stored as individual files in memory. If VVPAT enabled, ballot selections can be verified by viewing the enclosed printer tape at the right of the touchscreen. At the close of the polls, the stored votes are summarized and a tally tape is printed. When a machine is set to post-election mode, it writes its internal memory to flash memory on a PCMCIA card and the printed log of voting can be printed if necessary. The PCMCIA card and any printed record are taken from each machine to a central tabulation facility, where they are read into a central computer database where precinct results are aggregated. For remote facilities, votes are transmitted via a closed intranet, or internet channel [12].

The TSX runs Microsoft Windows CE Version 4.1, with modifications and it contains much of the same hardware as a 32-bit PC, including: a 32-bit Intel xScale processor, 32 MB of internal flash memory, and 64 MB RAM. The TSX contains a custom bootloader and other low-level support software. Applications such as BallotStation run on top of the OS and serve as the user interface. BallotStation interacts with the voter, accepts and records votes, counts the votes, and performs all other election-related processing [12]. It is possible that one of these systems was compromised with a Hursti attack in Florida, during the 2000 election, resulting in a negative number of votes for a candidate. Exploits for Microsoft CE can be found online and an attacker could leverage them to gain access to the system or to corrupt BallotStation to alter the election definition files or the order that information is displayed to users. In this manner, an attacker could redirect all votes from a popular candidate to a less popular one, just by switching the position of the names on the screen.

Sequoia/ Dominion

AVC Advantage

The AVC Advantage is a full-face DRE system with a touch-sensitive matrix of switches. Machines are activated from an operator panel on the side of the machine. The operator panel contains control buttons and an LCD alphanumeric display with two rows of 24 characters each. During an election, a poll-worker presses one such control button to allow each voter to vote. This is a serious security flaw because an unobserved voter could press the button and cast multiple votes. Votes are selected via switches and internally recorded to battery powered RAM. The switches on the display are oriented to correspond to a paper ballot overlay on the display. Internally, the correlation between voter selection and results is managed by proprietary software. Consequently, malware, software bugs, and numerous other errors can result in incorrect totals and results. Even if the system had an audit trail, the audit trail may be made consistent with the falsified results. At the close of polls, the system prints a paper summary of candidate totals and it writes ballot images to a Results Cartridge that resembles a VCR tape. The information on the cartridge is then either physically transported to a central tabulation facility or transmitted via modem, a cartridge reader, and a telephone line, depending on local election procedure and regulations. The total and ballot images are also stored in internal memory. The information can be extracted via the menu buttons on the operator panel. At the tabulation facility, all votes are read into tabulation databases and aggregated into a tally [12].

The memory cartridges of the AVC Advantage can be compromised. Voters can break physical security to access operator controls, unless an objective poll-worker is standing nearby. If the incorrect style of ballot is used, the machine will not correctly tally results. Finally, the disability access panel, or ADA interface, can be used to inject malware onto the system [12].

AVC Edge & AVC Edge II

The AVC Edge is a multi-lingual DRE touchscreen system. Voters activate the machines with smart cards and the machines store ballots and tallies on removable internal PCMCIA cards. To prevent someone from casting multiple votes, the voter access card deactivates after voting and the voter returns it to a poll-worker. Poll-workers also use smart cards and a similar interface to access controls for testing, maintenance, and opening or closing the polls. After the election, the results are either physically transported to election headquarters or transmitted via a computer network. Consequently, the results can be interrupted or intercepted by an adversary with access to the network.

The back of the Edge unit contains a power switch, a switch to open and close the polls on that particular voting machine, and a yellow "Activate" button. The Activate button can be used to switch the Edge into multiple operating modes and it can be exploited to allow a voter to cast multiple ballots. The back of the machine also features a small LCD screen that displays diagnostic and error messages. The Edge systems run on a proprietary operating system and it relies on proprietary firmware to control the hardware. The Edge contains three EEPROMs to store configuration information and ballot counters. One EEPROM acts as the configuration ROM and it contains information to identify the machine or customer and it contains a hardcoded cryptographic key or seed value. The other EEPROMs contain a public counter, which is reset at the start of each election, and a protective counter, which is incremented every time a vote is cast but is never reset across elections. Ballot definition and audio files to assist visually impaired voters are programmed on a WinEDS election management system server and stored on the Results Cartridge, which sits behind a small plastic door on the Edge. The Results Cartridge also stores the audit trail (ballot images, ballot summaries, etc.) and the event log. Event logging for the Edge is continuous and cannot be disabled. The audit log is also stored in internal audit memory. If the Results Cartridge is lost, damaged or destroyed, then it can be theoretically recovered from the internal audit memory. At the close of an election, the audit log can be printed on a VVPAT. The Edge is supported by Card Activators that encode or prepare smart cards for voter use. The Card Activators are programmed with ballot definitions and other information prior to the election. A Hybrid Activator and Accumulator (HAAT) can serve as an alternative to a card activator, to distribute ballot definitions. A HAAT also aggregates the votes from the machines at a polling place and transmits them to the central election office via a wireless cellular network [12]. An attacker could corrupt the card activators to prevent the use of smart cards, to alter definition files, or to distribute malware to multiple machines. A corrupted HAAT can be leveraged to alter definition files, alter results, access remote systems, or to spread malware to networked devices.

The 2007 California State Top to Bottom security review found significant security weaknesses throughout Sequoia systems. The software and firmware supporting the reviewed systems was not designed according to defensive software engineering or high-system assurance practices. Notably, they found that every software mechanism for transmitting election results and every software mechanism for updating software lacks reliable measures to detect or prevent tampering. There were numerous programming, logic, and architectural errors present in the software at the source code level.

Source code was found vulnerable to rudimentary flaws that facilitate buffer overflow attacks, format string vulnerabilities, and type mismatch errors, among other attacks. There were many instances of exception mishandling and several cases where the software did not behave according to documentation. The systems also lacked effective safeguards against corrupted or malicious data injected onto removable media, especially for devices entrusted to poll workers and other temporary staff with limited authority. This means that a threat actor could insert a corrupted memory unit or corrupted firmware chip into the unit and the change might not be noticed. The cryptography embedded in the systems can be easily circumvented because it is based on weak algorithms with known flaws or it is used in an insecure manner. The access controls are weak and an attacker could gain access to central vote counting computers or polling place equipment. In particular, security features and audit logs in the WinEDS backend system were ineffective against insider threats who could gain access to WinEDS systems or networks. Overall, in the short amount of time that security researchers reviewed Sequoia's code, they found an unsettling amount of exploitable vulnerabilities or fundamental errors, which reduced their overall trust in the system and its developer [20].

UniLect Corporation

UniLect Patriot and Peripheral Dynamics VMR 138

The Patriot is a DRE-touchscreen system that is networked to other Patriots and to a Precinct Control Unit (PCU) that contains election data via a removable InfoPack. Ballot information is transferred from city or county election officials to the polling places via an administrator interface and then loaded into the InfoPack via a connector called the InfoPacket. The Infopack is loaded into a PCU, it is tested, and then it is sealed and sent to the appropriate precinct. The (PCU) features an election worker control panel, a printer, an external emergency battery, the InfoPack, which contains the election files and final vote totals, and an internal modem for direct transfer of totals from a standard telephone in the precinct to the Patriot Central Station in the election office. Prior to the election, the PCU is set on a table and connected to each Patriot via a cable. The PCU is turned on and then an observed poll-worker breaks an “Open Polls” seal, opens the latch, and presses the red button within. A printer, the VMR 138, generates a report and all connected Patriot machines display all candidates with (hopefully) zero votes. After the election, the “Close Polls” seal is broken and the red button within is pressed. Copies of the final precinct reports are automatically printed. Vote data is stored in internal redundant memory during the election and is loaded into the PCU after the election. The information can be transmitted from there to a central tabulation center via modem, provided that poll-workers insert a line into a phone jack.

The Patriot is not networked to the internet, it has no operating system, and it has no attached keyboard or ports. This does not mean that the system is secure. An adversary could target the InfoPack. Vote totals can be manually edited by insiders at the Central Station. The log on both the PCU and the Central Station consists of a file of information. On the Central Station, the log is an unencrypted text file that is editable by the user. Worse, the log only records events that are initiated through the Patriot software. Functions performed through the Windows operating system interface, such as copying, deleting or substituting a file, are not logged at all. So another way of altering vote totals is to replace the totals file by another, an action which will not be logged. The precinct log maintained at the PCU does not record each voting event. Instead, it uses specific events, such as the opening or closing of polls. Logs can be made less susceptible to editing if they are written to write-once media, such as CD-R or paper printout [12].

Conclusion

The perpetuation of the illusion of security via obscurity must be immediately purged from the conversation each time voting officials and e-voting machine manufacturers attempt to debate the vulnerability arguments against their easily exploitable technologies. The question is not “Are script kiddies, lone-wolves, hacktivists, cyber-mercenaries, or nation-state actors from Russia or China trying to impact our elections?” Rather, due to our virtually defenseless election process, the questions that should be asked are “Why wouldn’t they?” and “How do we know that they have not already done so?” If the ambition of our adversaries was to do nothing more than spread distrust of the “establishment system” and introduce viral conspiracy theories to mainstream conversation, then they’ve garnered resounding success. Patriotism is rapidly being replaced by skepticism as the general population is now questioning the legitimacy of the democratic process. We send American’s to Iraq and Afghanistan to risk life, limb and death in order to spread and defend democracy abroad, yet we can’t even preserve the most sacred expression of the democratic process against enemies within our own boarders.

Without transparency in the design and operation of electronic voting systems, it is impossible to say with certainty that compromises have not occurred. As detailed in this report, security researchers have spent the past decade demonstrating that DRE and optical scanning systems from every manufacturer are vulnerable along numerous attack vectors. Instead of securing the systems, so far, the nation has relied on verified voter paper audit trails which in some cases may be just as susceptible to attack or may not ever be properly examined or considered. America switched from a paper ballot system to an electronic voting system for a reason. Paper ballots are much more susceptible to basic human error or to non-sophisticated insider threat than the electronic alternatives. Counting thousands or millions of paper ballots is difficult and impractical. That is not even considering that most recounts occur under the high pressure of a contentious election. Nearly every time there is a manual recount of the vote, the counting officials tabulate different numbers from the exact same pool of ballots. Often error bars of plus or minus so many votes are used to account for possible human counting errors. Intentional insider threats, such as an opinionated volunteer, may “misplace” or “alter” paper ballots. Again, the vulnerabilities and vulnerable systems discussed in this report are merely a fraction of the true electronic voting attack surface.

A portion of the trust in American democracy and freedom is eroded away with every exploitable vulnerability in every system which supports the democratic process. Without trust in the voting process, citizens cannot express their voices, they cannot choose their candidates, they cannot vote to defend their rights, and they cannot impart their rightfully given influence on the culture and trajectory of American Democracy. The preservation of the integrity of the democratic process rests on the expediency in which we respond to the hyper-evolving threat landscape in this digital age. Technologically mismanaged regional elections have national implications. The cyber, technical and physical vulnerabilities that riddle America's election process render a virtually limitless attack surface for adversaries who exploit it with infinite variations. Nation states, self-radicalized cyber lone wolves, hacktivists, cyber mercenaries and script kiddies all seek to interrupt, exploit and cripple American systems in every sector, and they are succeeding because the United States lacks the agility to bar technical intrusion, thwart the exfiltration and manipulation of data, prevent the theft of IP and PII, and forestall the incremental devastation to our critical infrastructures.

The very same personnel who manage regional elections, continuously fall for spear phishing attacks, watering hole exploits, and malvertising attacks, but they are placed in a space where cyber, technical and physical social engineering attacks are not only possible, but probable. Votes are tallied by voting officials without so much as a background check or cyber hygiene training and transmitted to the state to be tallied collectively by more officials with just as little or even less exploit defense comprehension. The entire system depends on electronic voting machines that have repeatedly been compromised by security researchers over the past decade. Nevertheless, these vulnerable systems that were developed without security-by-design, without foundational perimeter security, without transparency, and without oversight are still operational and will be used in the 2016 elections. Due to a lack of understanding and a dismissal of the evident threats demonstrated by notable security figures over the past decade, the conversation surrounding voting machine manipulation and hacking, is rendered to nothing more than an illusion of security; an ephemeral, topical facsimile of a much-needed conversation that is propped up just before and collapses soon after votes have been cast and tallied. Every election cycle, the conversation around voter fraud and e-voting machine exploitation comes into play a few months before and perhaps a few weeks after the presidential election. Due to the blatantly obvious cyber, technical and physical attack surface of local and state elections and as adversaries overtly exploit defenseless systems, could 2016 be the election cycle where Americans demand bi-partisan action for reform? This report and its companion documents aim to establish the need for substantial discussion of the topic, to loosely define the relevant attack surface, and to demonstrate the need to secure electronic voting systems.

Contact Information

Legislative & Executive Branch Inquiries:

- James Scott, Senior Fellow, ICIT (james@icitech.org, 202-774-0848)

Federal Agency & Underwriting Inquiries:

- Parham Eftekhari, Senior Fellow, ICIT (parham@icitech.org, 773-517-8534)

Links

Website: www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

https://www.facebook.com/ICITorg

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Sources

[1] L. Norden, "America’s Voting Machines at Risk," in Brennan Center for Justice, 2015. [Online]. Available: https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf. Accessed: Aug. 19, 2016.

[3] Dan Sinclair, "Lee County supervisor of elections short version," in YouTube, YouTube, 2016. [Online]. Available: https://www.youtube.com/watch?v=ROWNKpZY948. Accessed: Aug. 29, 2016.

[4] A. S. of State, "Temporary service interruption for voter view & VRAZII," Arizona Secretary of State, 2016. [Online]. Available: http://www.azsos.gov/about-office/media-center/azsosblog/948. Accessed: Aug. 30, 2016.

[5] D. Staahl, "Was Arizona’s voter database hacked? FBI says maybe," 2016. [Online]. Available: http://www.azfamily.com/story/32388223/fbi-trying-to-determine-if-arizona-voter-database-was-hacked. Accessed: Aug. 29, 2016. [6] D. Petrella, "Hackers penetrate Illinois voter registration database," The Southern, 2016. [Online]. Available: http://thesouthern.com/news/local/state-and-regional/hackers-penetrate-illinois-voter-registration-database/article_6e58f325-367f-5f8e-aa78-f0b8224865cd.html. Accessed: Aug. 29, 2016.

[7] M. Isikoff, "FBI says foreign hackers penetrated state election systems," 2016. [Online]. Available: https://www.yahoo.com/news/fbi-says-foreign-hackers-penetrated-000000175.html. Accessed: Aug. 29, 2016.

[8] R. Savransky, "FBI: Foreign hackers penetrated state election databases," TheHill, 2016. [Online]. Available: http://thehill.com/blogs/blog-briefing-room/news/293636-fbi-foreign-hackers-penetrated-state-election-databases. Accessed: Aug. 29, 2016.

[9] A. Sternstein, "Swing states reject feds’ offer to Cybersecure voting machines," Defense One, 2016. [Online]. Available: http://www.defenseone.com/technology/2016/08/want-dhs-help-secure-your-voting-machines-some-states-say-no/131052/. Accessed: Aug. 29, 2016.

[10] K. O. Hubler and W. Underhill, "Voting system standards, testing and certification," 2015. [Online]. Available: http://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx. Accessed: Aug. 29, 2016.

[11] S. Brain, "Voting turnout statistics," in Government, Statistic Brain, 2016. [Online]. Available: http://www.statisticbrain.com/voting-statistics/. Accessed: Aug. 29, 2016.

[12] "Verified voting," Verified Voting, 2014. [Online]. Available: https://www.verifiedvoting.org/. Accessed: Aug. 23, 2016.

[13] Report to the Office of the Attorney General: Avante Vote-Trakker Voter-verified Paper Record System Assessment, 1st ed. New Jersey: State of New Jersey, 2016, pp. 5-6. http://www.state.nj.us/state/elections/voter-critertia/vvpr-hearing-reports-06-07-08/NJIT-Avante-report-7.07.pdf.

[14] Commonwealth Security and Risk Management: Security Assessment of WinVote Voting Equipment for Department of Elections, 1st ed. Virginia Information Technologies Agency, 2016, pp. 2-7.elections.virginia.gov/WebDocs/VotingEquipReport/WINVote-final.pdf

[15] ClearAccess 1.0 Security Specification, 1st ed. State of Colorado, 2015, p. 6. https://www.sos.state.co.us/pubs/elections/VotingSystems/systemsDocumentation/ClearBallot/ClearAccess/ClearAccessSecuritySpecification-r.pdf.

[16] Siefers, Analysis of a Danaher / Shouptronic 1242 Electronic Voting Machine, 1st ed. Lehigh University, 2008, pp. 3-4.http://perfect.cse.lehigh.edu/Documents/JoeSiefersReportSpring2008.pdf.

[17] SECURITY ASSESSMENT SUMMARY REPORT FOR DOMINION VOTING SYSTEMS DEMOCRACY SUITE 4.0, 1st ed. United States EAC, 2016, pp. 9-13. http://www.eac.gov/assets/1/Documents/Security%20Assessment%20Report.pdf.

[18] D. Wallach, "California review of the ES&S AutoMARK and M100," 2008. [Online]. Available: https://freedom-to-tinker.com/blog/dwallach/california-review-esamps-automark-and-m100/. Accessed: Aug. 24, 2016.

[19] H. Harri, P. McDaniel and B. Matt, EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing, 1st ed. Office of Ohio Secretary of State, 2007, pp. 1-45. www.sos.state.oh.us/sos/info/EVEREST/00-SecretarysEVERESTExecutiveReport.pdf

[20] Top-to-Bottom Review | California Secretary of State", Sos.ca.gov, 2007. [Online]. Available: http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/. [Accessed: 24- Aug-2016].

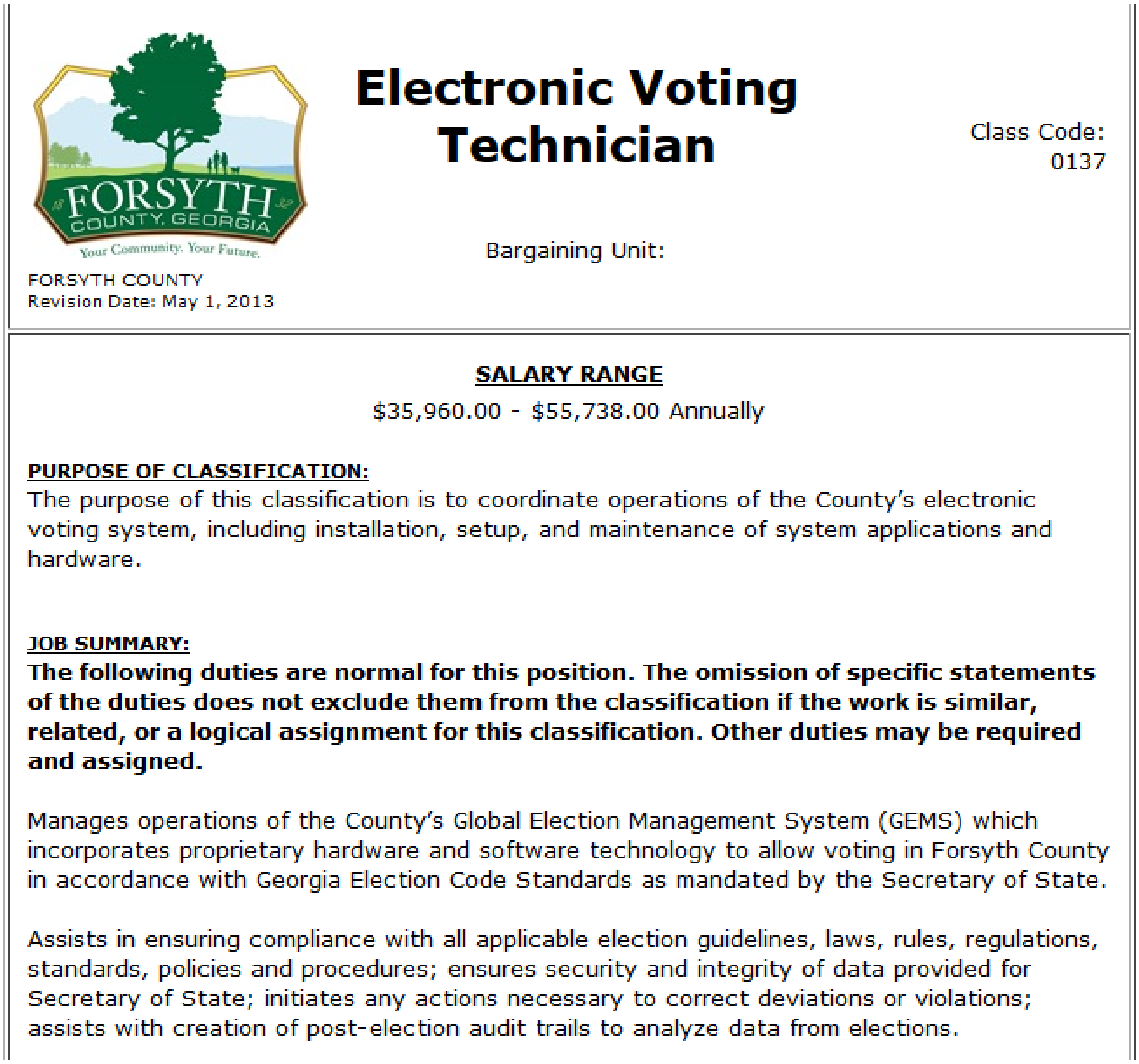
[21] "Election advisory no. 2012-03 - electronic voting system procedures," in Texas Secretary of State, 2012. [Online]. Available: http://www.sos.state.tx.us/elections/laws/advisory2012-03.shtml. Accessed: Sep. 7, 2016.

Appendix A: Electronic Voting Acronyms

ATI	Audio Tactile Interface
BOSS	Ballot Origination Software System
COTS	Consumer Off The Shelf
CVR	Cast Vote Record
DAU	Disabled Access Unit
DRE	Direct Recording Electronic
EAC	Election Assistance Commission
eCM	eSlate Cryptographic Module
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMS	Election Management System
ERM	Election Reporting Manager
EVM	Electronic Voting Machine
FEC	Federal Election Commission
GEMS	Global Election Management System
HAAT	Hybrid Activator and Accumulator
HAVA	Help America Vote Act (2002)
ICC	ImageCast Central
ICE	ImageCast Evolution
ICP	ImageCast Precinct
JBC	Judge’s Booth Controller
MBB	Mobile Ballot Box
NIST	National Institute for Standards and Technology
PBC	Precinct Ballot Counter
PCMCIA	Personal Computer Memory Card International Association
PCU	Precinct Control Unit
PEB	Personal Election Ballot
ROM	Read-Only Memory
RTAL	Real Time Audit Log
TGDC	Technical Guidelines Development Committee
VVPAT	Voter Verified Paper Audit Trail
VVPRS	Voter Verified Paper Record System
VVSG	Voluntary Voting System Guidelines

Appendix B: Sample Local and State Election Position Listings

Appendix B: Figure 1 - Forsyth County, Georgia Electronic Voting Technician



FORSYTH COUNTY
Revision Date: May 1, 2013

Electronic Voting Technician

Class Code: 0137

Bargaining Unit:

SALARY RANGE

$35,960.00 - $55,738.00 Annually

PURPOSE OF CLASSIFICATION:

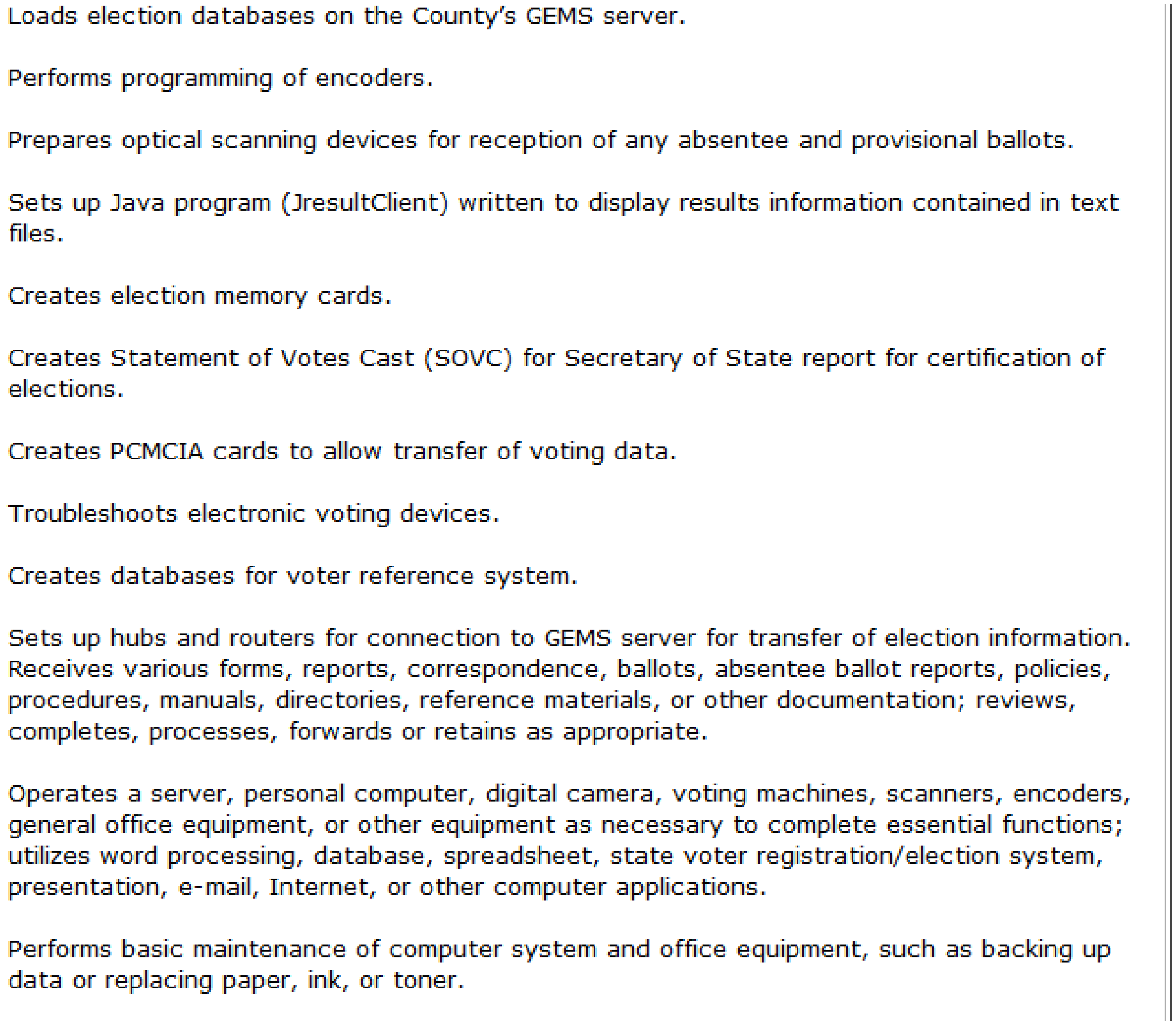
The purpose of this classification is to coordinate operations of the County's electronic voting system, including installation, setup, and maintenance of system applications and hardware.

JOB SUMMARY:

The following duties are normal for this position. The omission of specific statements of the duties does not exclude them from the classification if the work is similar, related, or a logical assignment for this classification. Other duties may be required and assigned.

Manages operations of the County's Global Election Management System (GEMS) which incorporates proprietary hardware and software technology to allow voting in Forsyth County in accordance with Georgia Election Code Standards as mandated by the Secretary of State.

Assists in ensuring compliance with all applicable election guidelines, laws, rules, regulations, standards, policies and procedures; ensures security and integrity of data provided for Secretary of State; initiates any actions necessary to correct deviations or violations; assists with creation of post-election audit trails to analyze data from elections.



Loads election databases on the County's GEMS server.

Performs programming of encoders.

Prepares optical scanning devices for reception of any absentee and provisional ballots.

Sets up Java program (JresultClient) written to display results information contained in text files.

Creates election memory cards.

Creates Statement of Votes Cast (SOVC) for Secretary of State report for certification of elections.

Creates PCMCIA cards to allow transfer of voting data.

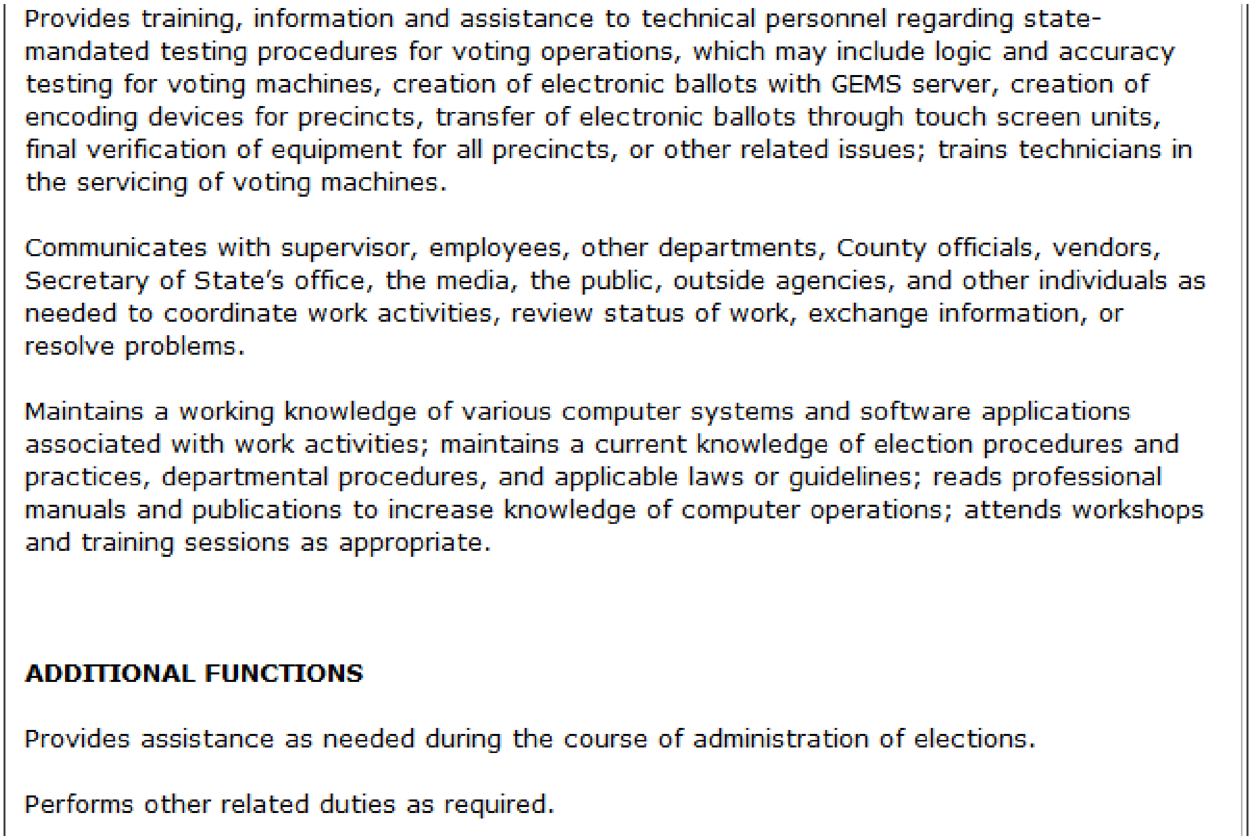
Troubleshoots electronic voting devices.

Creates databases for voter reference system.

Sets up hubs and routers for connection to GEMS server for transfer of election information. Receives various forms, reports, correspondence, ballots, absentee ballot reports, policies, procedures, manuals, directories, reference materials, or other documentation; reviews, completes, processes, forwards or retains as appropriate.

Operates a server, personal computer, digital camera, voting machines, scanners, encoders, general office equipment, or other equipment as necessary to complete essential functions; utilizes word processing, database, spreadsheet, state voter registration/election system, presentation, e-mail, Internet, or other computer applications.

Performs basic maintenance of computer system and office equipment, such as backing up data or replacing paper, ink, or toner.



Provides training, information and assistance to technical personnel regarding state-mandated testing procedures for voting operations, which may include logic and accuracy testing for voting machines, creation of electronic ballots with GEMS server, creation of encoding devices for precincts, transfer of electronic ballots through touch screen units, final verification of equipment for all precincts, or other related issues; trains technicians in the servicing of voting machines.

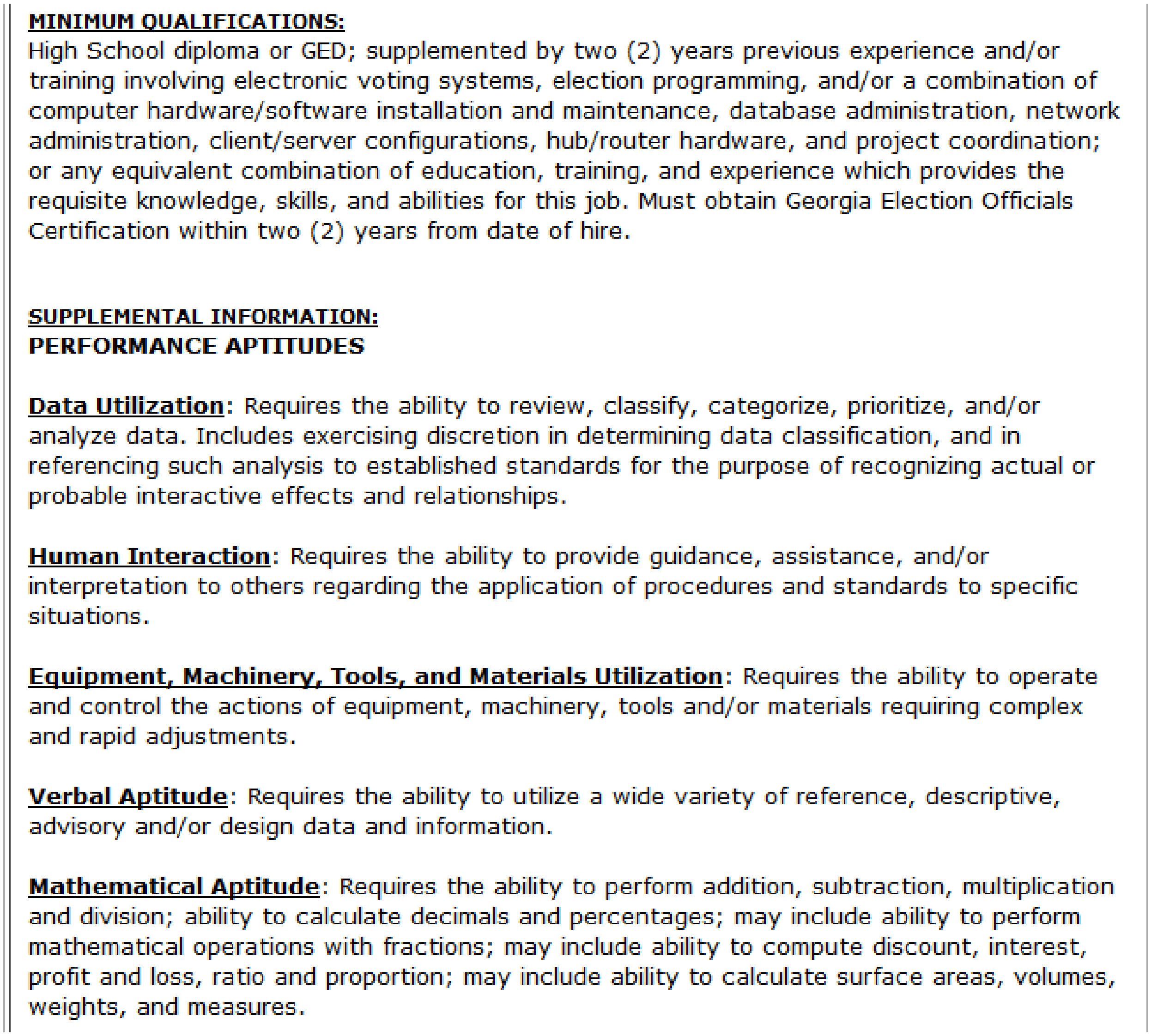
Communicates with supervisor, employees, other departments, County officials, vendors, Secretary of State's office, the media, the public, outside agencies, and other individuals as needed to coordinate work activities, review status of work, exchange information, or resolve problems.

Maintains a working knowledge of various computer systems and software applications associated with work activities; maintains a current knowledge of election procedures and practices, departmental procedures, and applicable laws or guidelines; reads professional manuals and publications to increase knowledge of computer operations; attends workshops and training sessions as appropriate.

ADDITIONAL FUNCTIONS

Provides assistance as needed during the course of administration of elections.

Performs other related duties as required.



MINIMUM QUALIFICATIONS:

High School diploma or GED; supplemented by two (2) years previous experience and/or training involving electronic voting systems, election programming, and/or a combination of computer hardware/software installation and maintenance, database administration, network administration, client/server configurations, hub/router hardware, and project coordination; or any equivalent combination of education, training, and experience which provides the requisite knowledge, skills, and abilities for this job. Must obtain Georgia Election Officials Certification within two (2) years from date of hire.

SUPPLEMENTAL INFORMATION:

PERFORMANCE APTITUDES

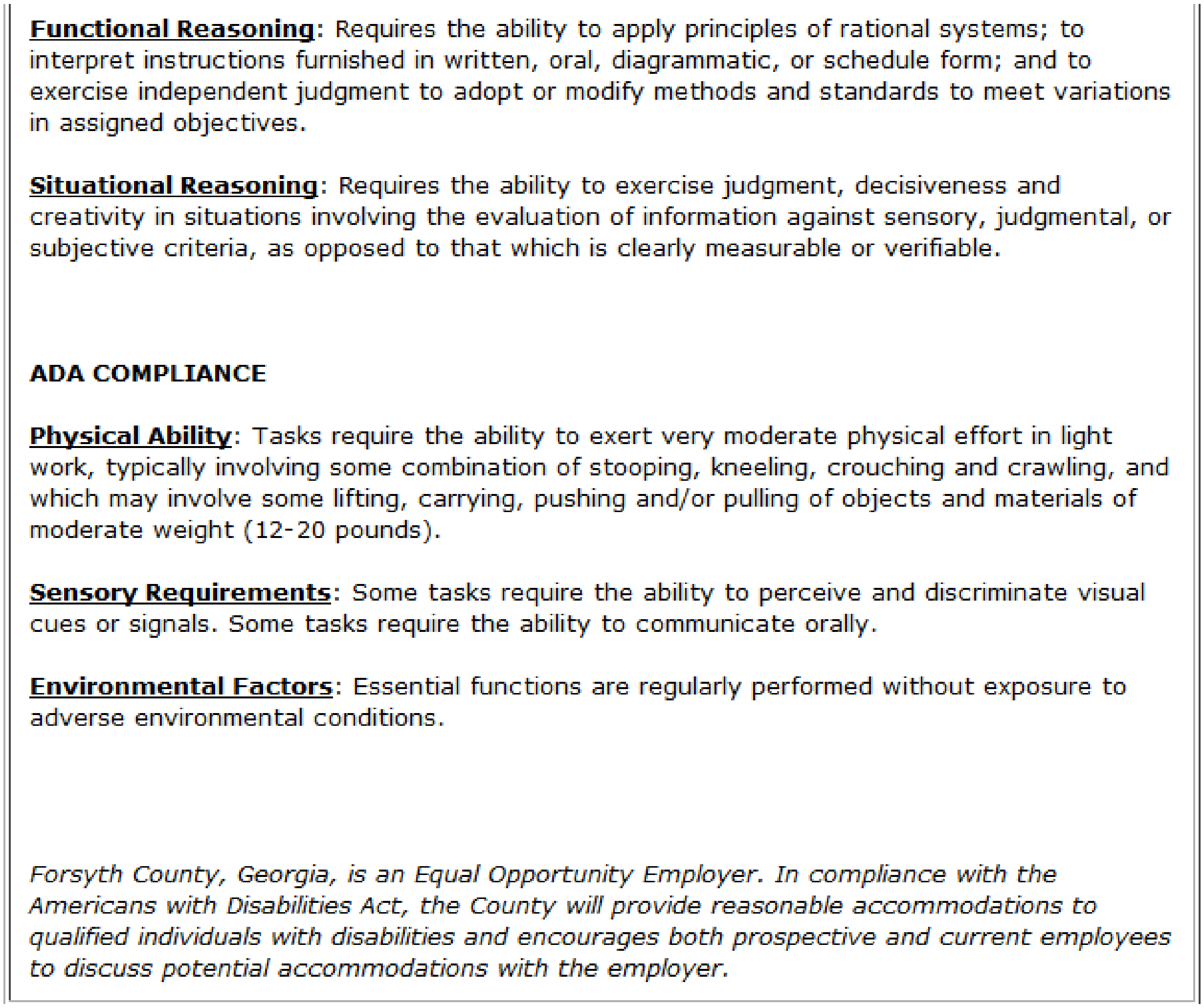
Data Utilization: Requires the ability to review, classify, categorize, prioritize, and/or analyze data. Includes exercising discretion in determining data classification, and in referencing such analysis to established standards for the purpose of recognizing actual or probable interactive effects and relationships.

Human Interaction: Requires the ability to provide guidance, assistance, and/or interpretation to others regarding the application of procedures and standards to specific situations.

Equipment, Machinery, Tools, and Materials Utilization: Requires the ability to operate and control the actions of equipment, machinery, tools and/or materials requiring complex and rapid adjustments.

Verbal Aptitude: Requires the ability to utilize a wide variety of reference, descriptive, advisory and/or design data and information.

Mathematical Aptitude: Requires the ability to perform addition, subtraction, multiplication and division; ability to calculate decimals and percentages; may include ability to perform mathematical operations with fractions; may include ability to compute discount, interest, profit and loss, ratio and proportion; may include ability to calculate surface areas, volumes, weights, and measures.



Functional Reasoning: Requires the ability to apply principles of rational systems; to interpret instructions furnished in written, oral, diagrammatic, or schedule form; and to exercise independent judgment to adopt or modify methods and standards to meet variations in assigned objectives.

Situational Reasoning: Requires the ability to exercise judgment, decisiveness and creativity in situations involving the evaluation of information against sensory, judgmental, or subjective criteria, as opposed to that which is clearly measurable or verifiable.

ADA COMPLIANCE

Physical Ability: Tasks require the ability to exert very moderate physical effort in light work, typically involving some combination of stooping, kneeling, crouching and crawling, and which may involve some lifting, carrying, pushing and/or pulling of objects and materials of moderate weight (12-20 pounds).

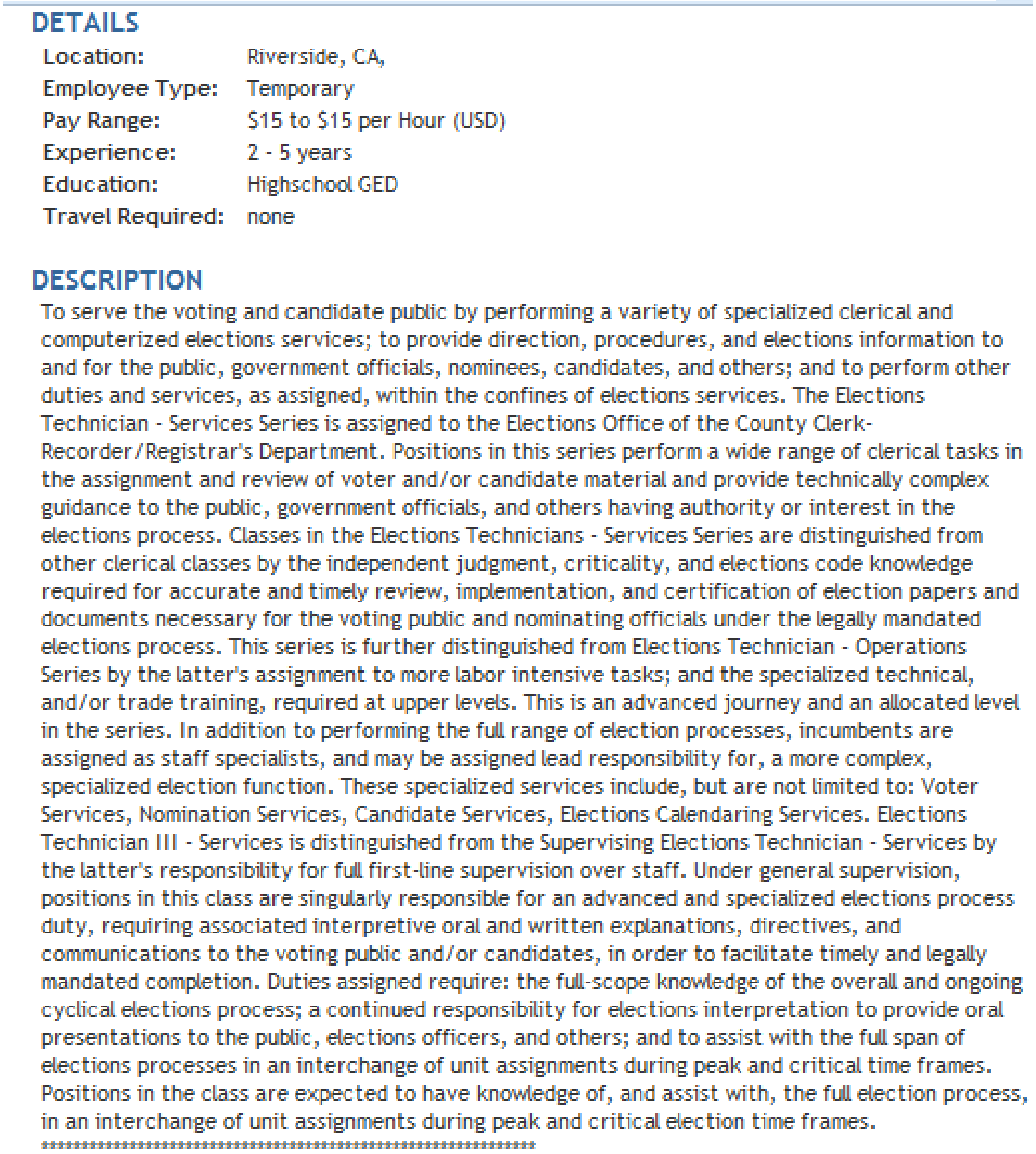
Sensory Requirements: Some tasks require the ability to perceive and discriminate visual cues or signals. Some tasks require the ability to communicate orally.

Environmental Factors: Essential functions are regularly performed without exposure to adverse environmental conditions.

Forsyth County, Georgia, is an Equal Opportunity Employer. In compliance with the Americans with Disabilities Act, the County will provide reasonable accommodations to qualified individuals with disabilities and encourages both prospective and current employees to discuss potential accommodations with the employer.

http://agency.governmentjobs.com/forsyth/default.cfm?action=specbulletin&ClassSpecID=789405&headerfooter=0

Appendix B: Figure 2 - Riverside, California Temporary Election Technician Position



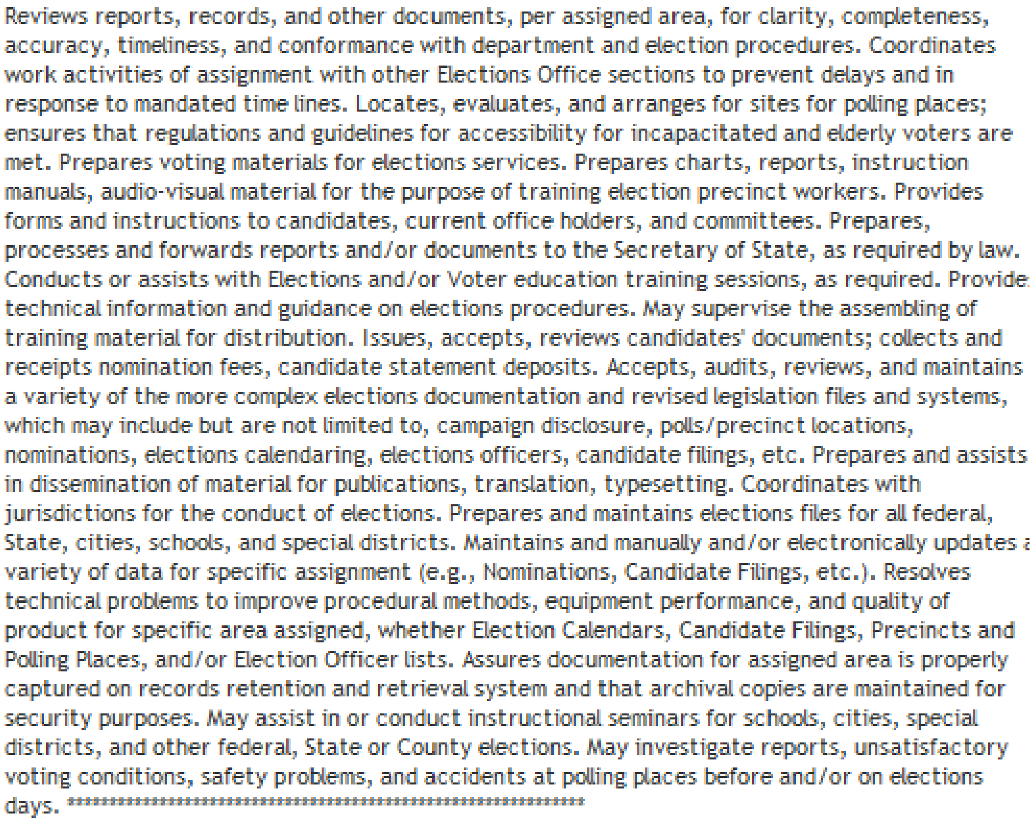
DETAILS

Location:	Riverside, CA,
Employee Type:	Temporary
Pay Range:	$15 to $15 per Hour (USD)
Experience:	2 - 5 years
Education:	Highschool GED
Travel Required:	none

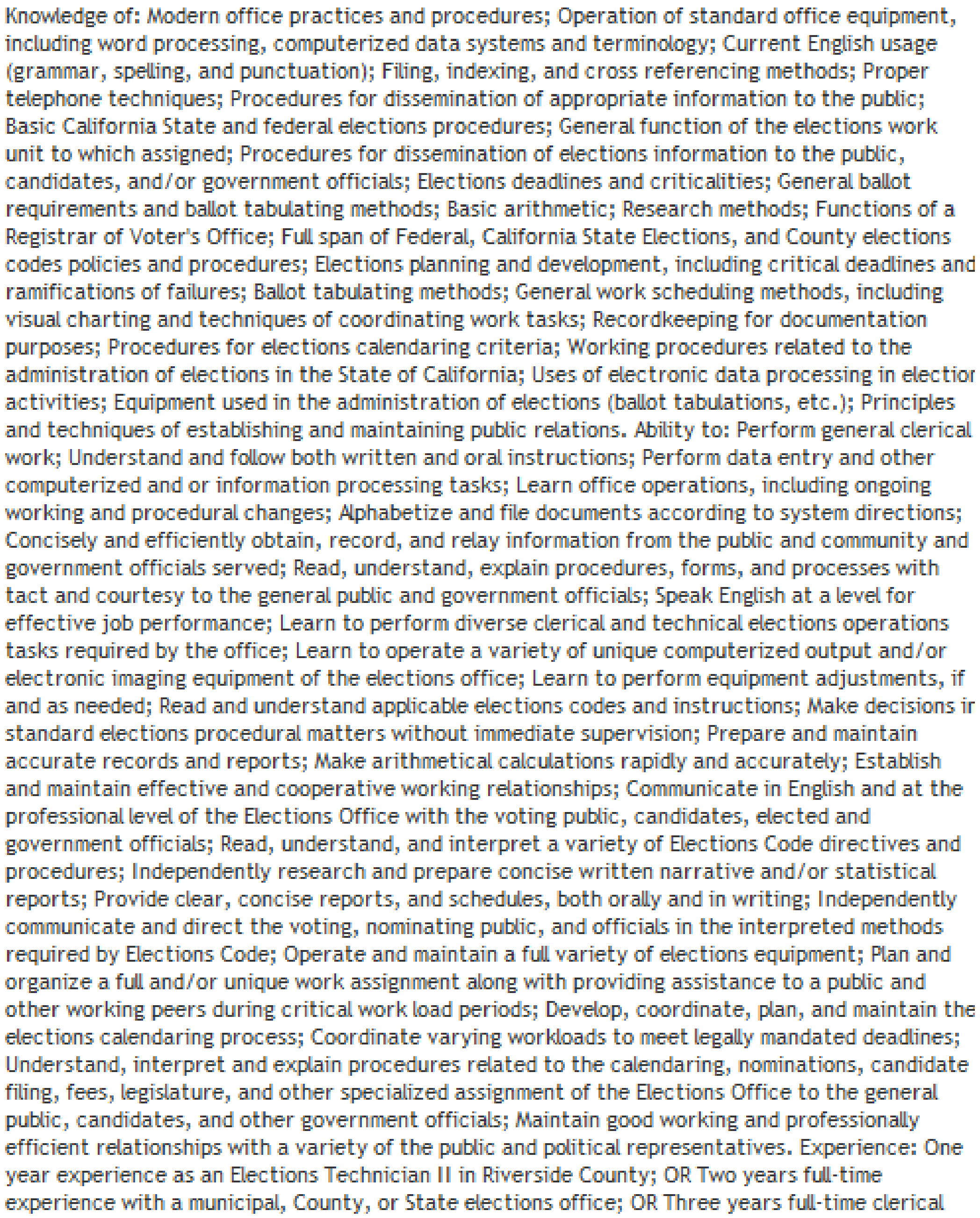
DESCRIPTION

To serve the voting and candidate public by performing a variety of specialized clerical and computerized elections services; to provide direction, procedures, and elections information to and for the public, government officials, nominees, candidates, and others; and to perform other duties and services, as assigned, within the confines of elections services. The Elections Technician - Services Series is assigned to the Elections Office of the County Clerk-Recorder/Registrar's Department. Positions in this series perform a wide range of clerical tasks in the assignment and review of voter and/or candidate material and provide technically complex guidance to the public, government officials, and others having authority or interest in the elections process. Classes in the Elections Technicians - Services Series are distinguished from other clerical classes by the independent judgment, criticality, and elections code knowledge required for accurate and timely review, implementation, and certification of election papers and documents necessary for the voting public and nominating officials under the legally mandated elections process. This series is further distinguished from Elections Technician - Operations Series by the latter's assignment to more labor intensive tasks; and the specialized technical, and/or trade training, required at upper levels. This is an advanced journey and an allocated level in the series. In addition to performing the full range of election processes, incumbents are assigned as staff specialists, and may be assigned lead responsibility for, a more complex, specialized election function. These specialized services include, but are not limited to: Voter Services, Nomination Services, Candidate Services, Elections Calendaring Services. Elections Technician III - Services is distinguished from the Supervising Elections Technician - Services by the latter's responsibility for full first-line supervision over staff. Under general supervision, positions in this class are singularly responsible for an advanced and specialized elections process duty, requiring associated interpretive oral and written explanations, directives, and communications to the voting public and/or candidates, in order to facilitate timely and legally mandated completion. Duties assigned require: the full-scope knowledge of the overall and ongoing cyclical elections process; a continued responsibility for elections interpretation to provide oral presentations to the public, elections officers, and others; and to assist with the full span of elections processes in an interchange of unit assignments during peak and critical time frames. Positions in the class are expected to have knowledge of, and assist with, the full election process, in an interchange of unit assignments during peak and critical time frames.

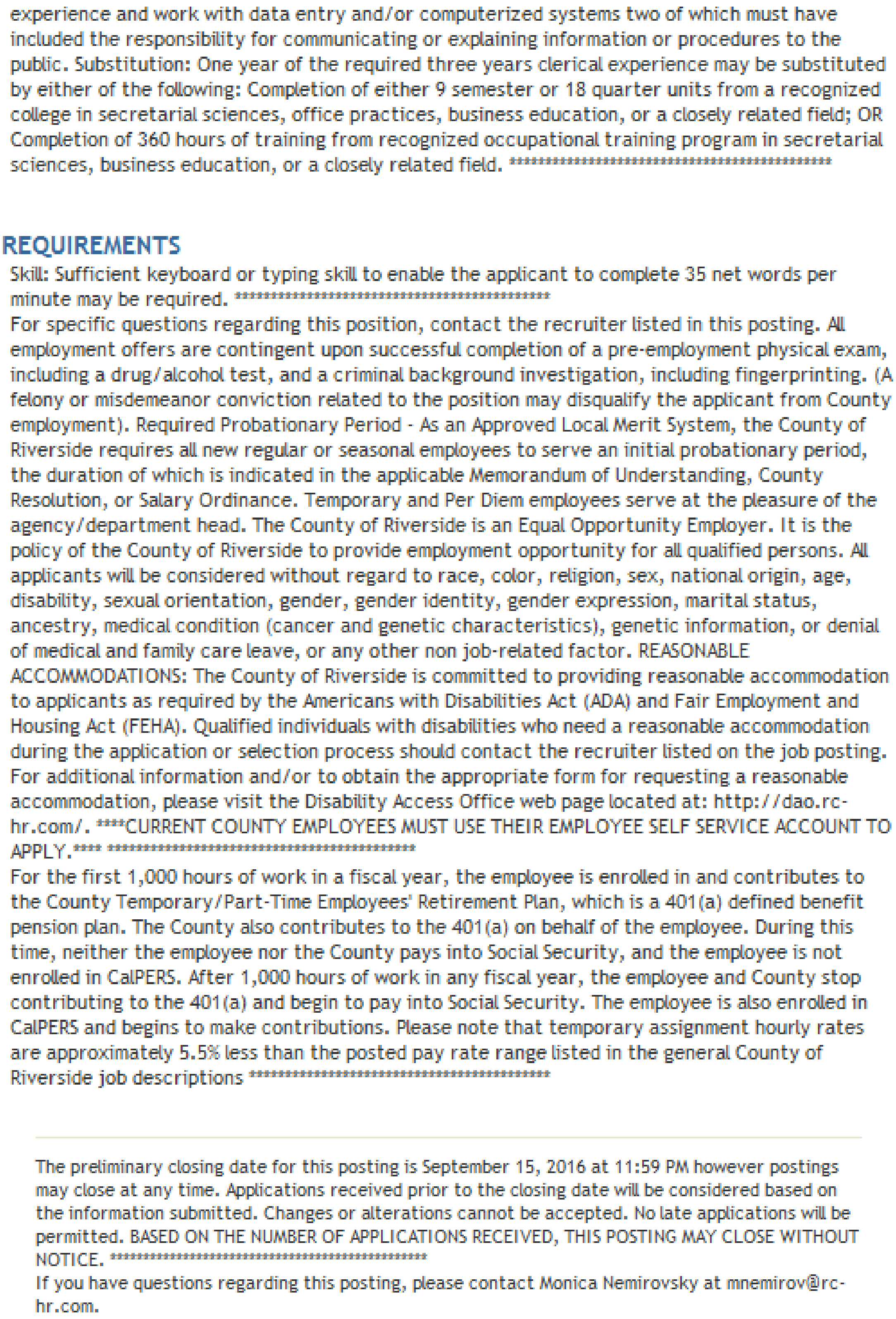
****



Reviews reports, records, and other documents, per assigned area, for clarity, completeness, accuracy, timeliness, and conformance with department and election procedures. Coordinates work activities of assignment with other Elections Office sections to prevent delays and in response to mandated time lines. Locates, evaluates, and arranges for sites for polling places; ensures that regulations and guidelines for accessibility for incapacitated and elderly voters are met. Prepares voting materials for elections services. Prepares charts, reports, instruction manuals, audio-visual material for the purpose of training election precinct workers. Provides forms and instructions to candidates, current office holders, and committees. Prepares, processes and forwards reports and/or documents to the Secretary of State, as required by law. Conducts or assists with Elections and/or Voter education training sessions, as required. Provides technical information and guidance on elections procedures. May supervise the assembling of training material for distribution. Issues, accepts, reviews candidates' documents; collects and receipts nomination fees, candidate statement deposits. Accepts, audits, reviews, and maintains a variety of the more complex elections documentation and revised legislation files and systems, which may include but are not limited to, campaign disclosure, polls/precinct locations, nominations, elections calendaring, elections officers, candidate filings, etc. Prepares and assists in dissemination of material for publications, translation, typesetting. Coordinates with jurisdictions for the conduct of elections. Prepares and maintains elections files for all federal, State, cities, schools, and special districts. Maintains and manually and/or electronically updates a variety of data for specific assignment (e.g., Nominations, Candidate Filings, etc.). Resolves technical problems to improve procedural methods, equipment performance, and quality of product for specific area assigned, whether Election Calendars, Candidate Filings, Precincts and Polling Places, and/or Election Officer lists. Assures documentation for assigned area is properly captured on records retention and retrieval system and that archival copies are maintained for security purposes. May assist in or conduct instructional seminars for schools, cities, special districts, and other federal, State or County elections. May investigate reports, unsatisfactory voting conditions, safety problems, and accidents at polling places before and/or on elections days. ***



Knowledge of: Modern office practices and procedures; Operation of standard office equipment, including word processing, computerized data systems and terminology; Current English usage (grammar, spelling, and punctuation); Filing, indexing, and cross referencing methods; Proper telephone techniques; Procedures for dissemination of appropriate information to the public; Basic California State and federal elections procedures; General function of the elections work unit to which assigned; Procedures for dissemination of elections information to the public, candidates, and/or government officials; Elections deadlines and criticalities; General ballot requirements and ballot tabulating methods; Basic arithmetic; Research methods; Functions of a Registrar of Voter's Office; Full span of Federal, California State Elections, and County elections codes policies and procedures; Elections planning and development, including critical deadlines and ramifications of failures; Ballot tabulating methods; General work scheduling methods, including visual charting and techniques of coordinating work tasks; Recordkeeping for documentation purposes; Procedures for elections calendaring criteria; Working procedures related to the administration of elections in the State of California; Uses of electronic data processing in electior activities; Equipment used in the administration of elections (ballot tabulations, etc.); Principles and techniques of establishing and maintaining public relations. Ability to: Perform general clerical work; Understand and follow both written and oral instructions; Perform data entry and other computerized and or information processing tasks; Learn office operations, including ongoing working and procedural changes; Alphabetize and file documents according to system directions; Concisely and efficiently obtain, record, and relay information from the public and community and government officials served; Read, understand, explain procedures, forms, and processes with tact and courtesy to the general public and government officials; Speak English at a level for effective job performance; Learn to perform diverse clerical and technical elections operations tasks required by the office; Learn to operate a variety of unique computerized output and/or electronic imaging equipment of the elections office; Learn to perform equipment adjustments, if and as needed; Read and understand applicable elections codes and instructions; Make decisions ir standard elections procedural matters without immediate supervision; Prepare and maintain accurate records and reports; Make arithmetical calculations rapidly and accurately; Establish and maintain effective and cooperative working relationships; Communicate in English and at the professional level of the Elections Office with the voting public, candidates, elected and government officials; Read, understand, and interpret a variety of Elections Code directives and procedures; Independently research and prepare concise written narrative and/or statistical reports; Provide clear, concise reports, and schedules, both orally and in writing; Independently communicate and direct the voting, nominating public, and officials in the interpreted methods required by Elections Code; Operate and maintain a full variety of elections equipment; Plan and organize a full and/or unique work assignment along with providing assistance to a public and other working peers during critical work load periods; Develop, coordinate, plan, and maintain the elections calendaring process; Coordinate varying workloads to meet legally mandated deadlines; Understand, interpret and explain procedures related to the calendaring, nominations, candidate filing, fees, legislature, and other specialized assignment of the Elections Office to the general public, candidates, and other government officials; Maintain good working and professionally efficient relationships with a variety of the public and political representatives. Experience: One year experience as an Elections Technician II in Riverside County; OR Two years full-time experience with a municipal, County, or State elections office; OR Three years full-time clerical



experience and work with data entry and/or computerized systems two of which must have included the responsibility for communicating or explaining information or procedures to the public. Substitution: One year of the required three years clerical experience may be substituted by either of the following: Completion of either 9 semester or 18 quarter units from a recognized college in secretarial sciences, office practices, business education, or a closely related field; OR Completion of 360 hours of training from recognized occupational training program in secretarial sciences, business education, or a closely related field. ***

REQUIREMENTS

Skill: Sufficient keyboard or typing skill to enable the applicant to complete 35 net words per minute may be required. ***

For specific questions regarding this position, contact the recruiter listed in this posting. All employment offers are contingent upon successful completion of a pre-employment physical exam, including a drug/alcohol test, and a criminal background investigation, including fingerprinting. (A felony or misdemeanor conviction related to the position may disqualify the applicant from County employment). Required Probationary Period - As an Approved Local Merit System, the County of Riverside requires all new regular or seasonal employees to serve an initial probationary period, the duration of which is indicated in the applicable Memorandum of Understanding, County Resolution, or Salary Ordinance. Temporary and Per Diem employees serve at the pleasure of the agency/department head. The County of Riverside is an Equal Opportunity Employer. It is the policy of the County of Riverside to provide employment opportunity for all qualified persons. All applicants will be considered without regard to race, color, religion, sex, national origin, age, disability, sexual orientation, gender, gender identity, gender expression, marital status, ancestry, medical condition (cancer and genetic characteristics), genetic information, or denial of medical and family care leave, or any other non job-related factor. REASONABLE ACCOMMODATIONS: The County of Riverside is committed to providing reasonable accommodation to applicants as required by the Americans with Disabilities Act (ADA) and Fair Employment and Housing Act (FEHA). Qualified individuals with disabilities who need a reasonable accommodation during the application or selection process should contact the recruiter listed on the job posting. For additional information and/or to obtain the appropriate form for requesting a reasonable accommodation, please visit the Disability Access Office web page located at: http://dao.rc-hr.com/. ****CURRENT COUNTY EMPLOYEES MUST USE THEIR EMPLOYEE SELF SERVICE ACCOUNT TO APPLY.**** ***

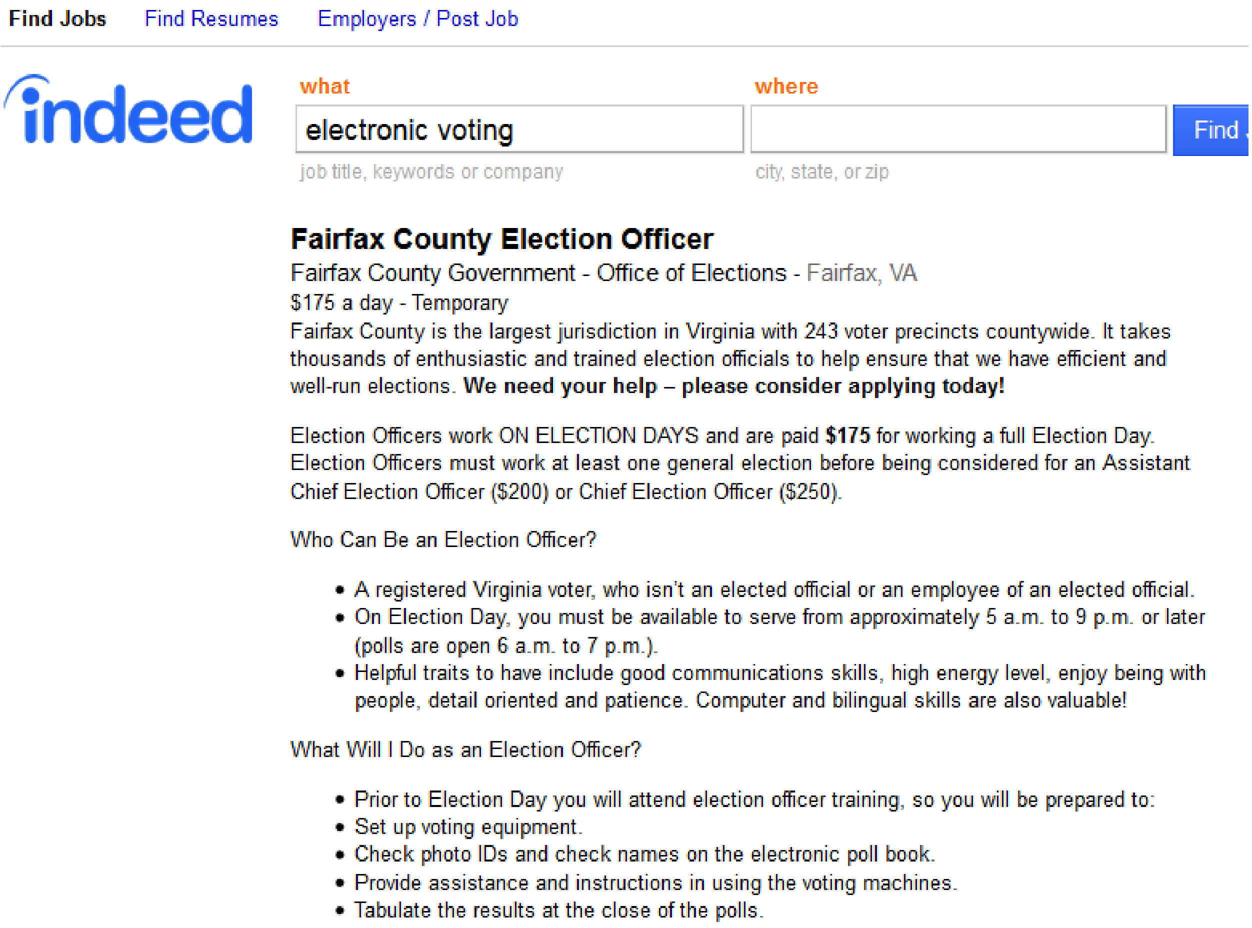
For the first 1,000 hours of work in a fiscal year, the employee is enrolled in and contributes to the County Temporary/Part-Time Employees' Retirement Plan, which is a 401(a) defined benefit pension plan. The County also contributes to the 401(a) on behalf of the employee. During this time, neither the employee nor the County pays into Social Security, and the employee is not enrolled in CalPERS. After 1,000 hours of work in any fiscal year, the employee and County stop contributing to the 401(a) and begin to pay into Social Security. The employee is also enrolled in CalPERS and begins to make contributions. Please note that temporary assignment hourly rates are approximately 5.5% less than the posted pay rate range listed in the general County of Riverside job descriptions ***

The preliminary closing date for this posting is September 15, 2016 at 11:59 PM however postings may close at any time. Applications received prior to the closing date will be considered based on the information submitted. Changes or alterations cannot be accepted. No late applications will be permitted. BASED ON THE NUMBER OF APPLICATIONS RECEIVED, THIS POSTING MAY CLOSE WITHOUT NOTICE. ***

If you have questions regarding this posting, please contact Monica Nemirovsky at mnemirov@rc-hr.com.

http://post.talemetry.com/onlinedisplay/jobdisplay.cfm?posting=1000123747&bid=326

Appendix B: Figure 3 - Fairfax County, Virginia Election Officer Position



what: electronic voting

Fairfax County Election Officer

Fairfax County Government - Office of Elections - Fairfax, VA

$175 a day - Temporary

Fairfax County is the largest jurisdiction in Virginia with 243 voter precincts countywide. It takes thousands of enthusiastic and trained election officials to help ensure that we have efficient and well-run elections. **We need your help – please consider applying today!**

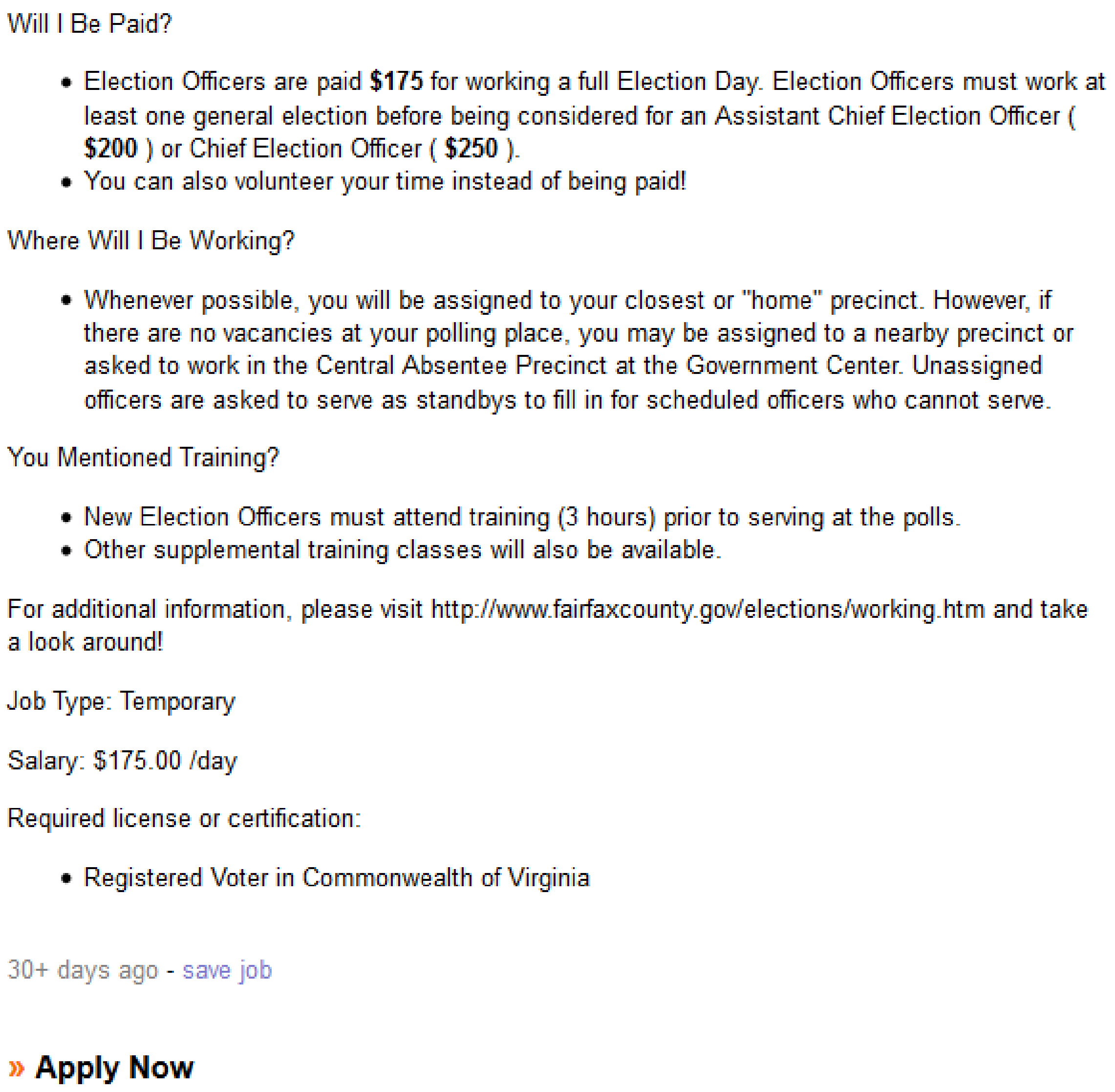
Election Officers work ON ELECTION DAYS and are paid **$175** for working a full Election Day. Election Officers must work at least one general election before being considered for an Assistant Chief Election Officer ($200) or Chief Election Officer ($250).

Who Can Be an Election Officer?

- A registered Virginia voter, who isn't an elected official or an employee of an elected official.
- On Election Day, you must be available to serve from approximately 5 a.m. to 9 p.m. or later (polls are open 6 a.m. to 7 p.m.).
- Helpful traits to have include good communications skills, high energy level, enjoy being with people, detail oriented and patience. Computer and bilingual skills are also valuable!

What Will I Do as an Election Officer?

- Prior to Election Day you will attend election officer training, so you will be prepared to:
- Set up voting equipment.
- Check photo IDs and check names on the electronic poll book.
- Provide assistance and instructions in using the voting machines.
- Tabulate the results at the close of the polls.



Will I Be Paid?

- Election Officers are paid **$175** for working a full Election Day. Election Officers must work at least one general election before being considered for an Assistant Chief Election Officer (**$200**) or Chief Election Officer (**$250**).
- You can also volunteer your time instead of being paid!

Where Will I Be Working?

- Whenever possible, you will be assigned to your closest or "home" precinct. However, if there are no vacancies at your polling place, you may be assigned to a nearby precinct or asked to work in the Central Absentee Precinct at the Government Center. Unassigned officers are asked to serve as standbys to fill in for scheduled officers who cannot serve.

You Mentioned Training?

- New Election Officers must attend training (3 hours) prior to serving at the polls.
- Other supplemental training classes will also be available.

For additional information, please visit http://www.fairfaxcounty.gov/elections/working.htm and take a look around!

Job Type: Temporary

Salary: $175.00 /day

Required license or certification:

- Registered Voter in Commonwealth of Virginia

30+ days ago - save job

http://www.indeed.com/cmp/Fairfax-County-Office-of-Elections/jobs/County-Election-Officer-f8b71754e380ea8a?sjdu=QwrRXKrqZ3CNX5W-O9jEvbBYWkx5vu7NAddotXjceWpZaCcUKZ53ZerBOcl_JsglRzpsoDdowz1SWPtefclPMHtifIpf3ULYVeSMhEb-2to

Appendix C: Summary of Electronic Voting Manufacturers by System, Type and Regions Used in 2016

Manufacturer	System	Type	Used in 2016
Avante	Vote-Trakker	DRE-Touchscreen (VVPAT Capable)	Warren County, New Jersey
Advanced Voting Systems (AVS)	WINVote	DRE-Touchscreen (No VVPAT)	No Longer in Use
	WINScan	Central Count Optical Scan	No Longer in Use
Clear Ballot Group	ClearVote	Optical Scan with Ballot Marking Device	Oregon (6 counties)
Danaher Controls	Danaher Shouptronic 1242 / ELECTronic 1242	DRE Pushbutton (No VVPAT)	Delaware (Statewide), Arkansas (2 counties), Pennsylvania (6 counties), and Tennessee (1 county)
DFM Associates	Mark-A-Vote	Optical Scan Paper Ballot	California (Lake Madera and Sonoma Counties)
Dominion Voting Systems	ImageCast Democracy Suite	Optical scan with digital imaging, an integrated ballot marking device, and an optional central count system	New Mexico (Statewide), Colorado (19 counties), Florida (9 counties), Iowa (3 counties), Louisiana (Statewide for absentee ballot tabulation), Massachusetts (municipalities in 10 counties), Missouri (13 counties), New Jersey (1 county), New York (52 counties), Ohio (4 counties), Tennessee (1 county), Virginia (11 localities), and Wisconsin (1 county)
Election Systems and Software (ES&S)	AutoMARK Voter Assist Terminal (VAT)	Assistive Ballot Marking Device	Alabama (Statewide), Idaho (Statewide), Massachusetts (Statewide), Michigan (Statewide), Minnesota (Statewide), Montana (Statewide), Nebraska (Statewide), North Dakota (Statewide), Rhode Island (Statewide), South Dakota (Statewide), Arizona (2 counties), California (13 counties), Florida (24 counties), Illinois (45 jurisdictions), Indiana (5 counties), Iowa (38 counties), Kansas (58 counties), Mississippi (4 counties), Missouri (14 counties), New York (5 counties and all 5 New York City boroughs), North Carolina (68 counties), Ohio (33 counties), Pennsylvania (13 counties), Texas (97 counties), Virginia (22 localities), Washington (11 counties), West Virginia (4 counties), Wisconsin (23 counties), and Wyoming (20 counties)

Manufacturer	System	Type	Used in 2016
	DS200	Precinct Count Optical Scan with digital image	Maryland (Statewide), Alabama (54 counties), Arizona (2 counties), Arkansas (5 counties), Florida (38 counties), Idaho (10 counties), Illinois(6 jurisdictions), Indiana (1 county), Iowa (1 county), Kansas (1 county), Maine (some towns in all counties), Massachusetts (5 counties), Minnesota (3 counties), Mississippi (1 county), Missouri (1 county), Montana (5 counties), New York (5 counties and all five New York City boroughs), North Carolina (3 counties), Ohio (9 counties), Tennessee (2 counties), Virginia (23 localities), West Virginia (2 counties), and Wisconsin (9 counties).
	DS850	Central Count Optical Scan with digital image	Maryland (Statewide), Arizona (5 counties), Florida (18 counties), Idaho (1 county), Indiana (1 county), Minnesota (3 counties), Missouri (1 county), Montana (7 counties), Nebraska (1 county), New York (1 county), Ohio (1 county), Oregon (3 counties), South Dakota (5 counties), Texas (1 county), and Virginia (1 locality)
	ExpressVote	Ballot Marking Device (VVPAT Capable)	Maine (Statewide), Maryland (Statewide), Arizona (4 counties), Arkansas (5 counties), Florida (9 counties), Idaho (7 counties), Indiana (1 county), Kansas (1 county), Missouri (1 county), Ohio (2 counties), Tennessee (1 county), Virginia (19 localities), West Virginia (2 counties), and Wisconsin (1 county)
	InkaVote	Optical Scan	California (Los Angeles County)
	iVotronic	DRE-Touchscreen (VVPAT Capable with the Real Time Audit Log (RTAL) printer)	**(With VVPAT):** Arkansas (68 counties), Colorado (1 county), the District of Columbia, Kansas (6 counties), Missouri (1 county), North Carolina (36 counties), Ohio (7 counties), West Virginia (49 counties), and Wisconsin (2 counties) **(Without VVPAT):** South Carolina (Statewide), Colorado (1 county), Florida (7 counties), Indiana (10 counties), Kansas (13 counties), Kentucky (22 counties), Mississippi (1 county), New Jersey (1 county), Pennsylvania (26 counties), Tennessee (16 counties), Texas (46 counties), and Virginia (4 localities).

Manufacturer	System	Type	Used in 2016
	Model 100	Precinct Count Optical Scan	Alabama (13 counties), Arizona (1 county), Arkansas (33 counties), California (9 counties), Colorado (2 counties), the District of Columbia, Florida (2 counties), Idaho (5 counties) , Illinois (36 jurisdictions), Indiana (3 counties), Iowa (17 counties), Kansas (45 counties), Kentucky (22 counties), Michigan (18 counties), Minnesota (80 counties), Mississippi (4 counties), Missouri (5 jurisdictions), Montana (26 counties), Nebraska (36 counties), North Carolina (92 counties), North Dakota (53 counties), Ohio (27 counties), Pennsylvania (14 counties), South Carolina (36 counties), South Dakota (31 counties), Tennessee (9 counties), Texas (78 counties), Virginia (7 localities), West Virginia (3 counties), Wisconsin (11 counties), and Wyoming (20 counties)
	Models 150	Central Count Optical Scan	Montana (1 county), New Jersey (1 county), and Tennessee (1 county)
	Model 550	Central Count Optical Scan	New Jersey (2 counties)
	Model 650	Central Count Optical Scan	Arizona (1 county), Arkansas (24 counties), California (6 counties), Colorado (1 county), the District of Columbia, Florida (10 counties), Idaho (13 counties), Illinois (1 county), Indiana (2 counties), Kansas (30 counties), Minnesota (2 counties), Missouri (12 jurisdictions), Montana (12 counties), Nebraska (56 counties), New Jersey (1 county), North Carolina (11 counties), North Dakota (3 counties), Ohio (12 counties), Oregon (22 counties), Pennsylvania (6 counties), South Carolina (10 counties), South Dakota (30 counties), Tennessee (2 counties), Texas (67 counties), Washington (11 counties), West Virginia (18 counties), and Wyoming (6 counties)
	Optech IIIP (3P) Eagle	Precinct Count Optical Scan	Rhode Island (Statewide), Indiana (6 counties), Massachusetts (some towns in 9 counties), New Jersey (1 county), Virginia (10 localities), and Wisconsin (municipalities in 27 counties)
	Votamatic	Punch Card Paper Ballot	Not Used in 2016 Election

Manufacturer	System	Type	Used in 2016
Hart Intercivic	Ballot Now	Central Count Optical Scan	California (5 counties), Colorado (9 counties), Oregon (3 counties), Tennessee (4 counties), Texas (36 counties), Virginia (1 locality), and Washington (1 county).
	eScan and eScan AT	Precinct Count Optical Scan with digital imaging	Hawaii (Statewide) Oklahoma (Statewide), California (2 counties), Colorado (29 counties), Idaho (3 counties), Indiana (6 counties), Kentucky (98 counties), Ohio (2 counties), Pennsylvania (3 counties), Tennessee (25 counties), Texas (53 counties), Virginia (1 locality), and Washington (20 counties)
	Verity Voting System	Precinct Count Optical Scan with digital imaging and an integrated Ballot Marking Device and optional Central Count Optical Scan system.	Idaho (1 county), Minnesota (1 county), Oregon (1 county), Virginia (6 localities), and Washington (1 county)
	eSlate	DRE-Dial (VVPAT Capable with VBO Printer)	**(With VVPAT):** Hawaii (Statewide), California (8 counties), Colorado (40 counties), Idaho (2 counties), Illinois (3 counties), Ohio (2 counties), and Washington (21 counties). **(Without VVPAT):** Indiana (6 counties), Kentucky (97 counties), Pennsylvania (4 counties), Tennessee (31 counties), Texas (103 counties), and Virginia (3 localities)
IVS LLC	Inspire Vote-By-Phone	Telephone-based Assistive Ballot Marking Device	Connecticut (Statewide) and Vermont (Statewide)
Microvote General Corporation	Chatsworth ACP-2200 and OMR-9002	Central Count Optical Scan	Indiana (48 counties) and Tennessee. (44 counties)
	Infinity	DRE-Pushbutton	Indiana (47 counties) and Tennessee (46 counties)

Manufacturer	System	Type	Used in 2016
Populex	PopulexSlate	Digital Ballot Marker	Missouri (Worth County)
Premier/ Diebold	AccuVote OS/ ES 2000	Precinct Count Optical Scan	Connecticut (Statewide), and Utah (used statewide for mail ballot tabulation), Georgia (used statewide for mail ballot tabulation), Alaska (many jurisdictions statewide), Massachusetts (many jurisdictions statewide), New Hampshire (many jurisdictions statewide), Vermont (many jurisdictions statewide), Arizona (6 counties), California (16 counties), Colorado (11 counties), Florida16 counties , Illinois (64 jurisdictions), Indiana (20 counties), Iowa (13 counties), Kansas (25 counties), Kentucky (1 county), Michigan (37 counties), Minnesota (1 county), Mississippi (74 counties, primarily for absentee ballots), Missouri (42 jurisdictions), Ohio (37 counties), Tennessee (1 county), Texas (5 counties), Virginia (20 localities), Washington (1 county), Wisconsin (municipalities in 13 counties), and Wyoming (3 counties)
	AccuVote OSX	Precinct Count Optical Scan with digital imaging	Iowa (8 counties) and Ohio (4 counties)
	AccuVote OS Central Count Scanner	Central Count Optical Scan Paper Ballot Voting System	Delaware (Statewide for absentee ballot tabulation), Arizona (1 county), California (11 counties), Florida (2 counties), and Iowa (8 counties)
	AccuVote TS & TSX	DRE-Touchscreen (VVPAT Capable with AccuView Printer)	**(with VVPAT):** Alaska (Statewide), Utah (Statewide), Arizona (7 counties), California (14 counties), Colorado (12 counties), Illinois (60 jurisdictions), Kansas (1 county), Mississippi (31 counties), Missouri (41 jurisdictions), Ohio (41 counties), Washington (1 county), Wisconsin (municipalities in 13 counties), and Wyoming (3 counties) **(without VVPAT):** Georgia (Statewide), Florida (16 counties), Indiana (20 counties), Kansas (25 counties) Kentucky (1 county), Mississippi (46 counties), Pennsylvania (16 counties), Tennessee (1 county), Texas (8 counties), and Virginia (10 localities)

Manufacturer	System	Type	Used in 2016
Sequoia/ Dominion	AVC Advantage	DRE-Pushbutton	Louisiana (Statewide), New Jersey (18 counties), Pennsylvania (2 counties) and Virginia (4 localities)
	AVC Edge & AVC Edge II	DRE-Touchscreen (VVPAT Capable with VeriVote printer)	**(With VVPAT):** Nevada (Statewide), Arizona (1 county), California (22 counties), Colorado (3 counties), Illinois (2 jurisdictions), Missouri (20 counties), Washington (5 counties), and Wisconsin (municipalities in 45 counties) **(Without VVPAT):** Louisiana (Statewide for early voting), Florida (2 counties), New Jersey (1 county), Pennsylvania (1 county), and Virginia (27 localities)
	Optech Insight	Precinct Count Optical Scan	Nevada (Statewide in for absentee ballot tabulation), Arizona (1 county), California (9 counties), Colorado (1 county), Florida (2 counties), Illinois (2 jurisdictions), Michigan (26 counties), Missouri (19 counties), and Wisconsin (municipalities in 18 counties)
	Optech 400-C/ IV-C/ Model 400	Central Count Optical Scan	Nevada (Statewide in for absentee ballot tabulation), Arizona (1 county), California (17 counties), Colorado (2 counties), Florida (2 counties), New Jersey (1 county), and Washington (5 counties)
UniLect Corporation	UniLect Patriot	DRE-Touchscreen	Virginia (21 localities)
	Peripheral Dynamics VMR 138	Central Count Optical Scan	Virginia (14 localities)
Unisyn Voting Solutions	OpenElect Voting Optical (OVO)	Optical Scan with digital imaging	Puerto Rico (Territory-wide), Arizona (3 counties), Indiana (3 counties), Iowa (58 counties), Kansas (1 county), Missouri (26 counties), Tennessee (1 county), and Virginia (22 localities)