Virginia Information Technologies Agency

VITA

NASCIO

Representing Chief Information Officers of the States

Fighting Election Fraud

Cybersecurity

Initiation date: August 2017

Completion date: December 2017

Nomination submitted by:
Nelson P. Moe
Chief Information Officer
Commonwealth of Virginia
Virginia Information Technologies Agency

2018 Commonwealth of Virginia NASCIO Award Submission
Project: Fighting Election Fraud
Virginia Information Technologies Agency (VITA) and Department of Elections
Category: Cybersecurity

Executive Summary

The Commonwealth of Virginia has 133 local election jurisdictions and more than five million registered voters. As in all states, maintaining the public's trust in the integrity of our elections is essential to the democratic process and homeland security. This critical need has been a topic of national and international conversation in recent months.

Virginia is a leader among states for its cybersecurity program and state network, and its voter registration system enjoys these significant protections. Still, the security of touchscreen direct-recording electronic (DRE) voting machines has been a concern. DREs process data by computer program and do not maintain a paper record of votes. After voting is over, DREs produce an electronic tabulation of votes on a memory card and print a paper summary of the results. Most DRE systems do not have a method to check whether the votes cast are the same as the vote count in the system. Once all votes are recorded, the machines send vote totals to the state's network for results reporting.

July 2017 news coverage cited breaches to voting machines made public at the annual hacker's DefCon cybersecurity conference. Given these security vulnerabilities, concerns emerged about protecting Virginia's information technology (IT) systems, commonwealth data and citizens' votes.

To address these concerns, the State Department of Elections (ELECT) asked the Virginia Information Technologies Agency (VITA)'s Commonwealth Security and Risk Management (CSRM) directorate to assess the state's voting machines. Following CSRM review, on Sept. 8, 2017, Virginia Commissioner of Elections Edgardo Cortés recommended to the State Board of Elections (SBE) decertification of all DREs. Affected localities were notified immediately.

Most localities using the machines were rural or urban areas with no funding to purchase new voting devices. Vendors worked with the commonwealth to equip localities with new machines. Two weeks prior to the November General election, all 22 localities had new voting equipment.

Previously, Advanced Voting Systems WINVote devices were tested by VITA in 2015. VITA recommended decertification based upon absent security protocols, weak passwords, and unpatched software, among other security risks.

With concerns about election fraud, this 2017 initiative aligned closely with the governor's priorities and CIO goals supporting cybersecurity, as well as citizens of the commonwealth, local government entities, advocacy groups, those seeking public office, VITA, ELECT and the SBE, among others.

Concept

In July 2017, the Wall Street Journal and other news outlets reported that hackers at the DefCon cybersecurity conference successfully compromised voting machines that were still is use throughout the United States for the election process. Prompted by these reports, ELECT asked VITA to conduct a security assessment of the following DRE touchscreen models: Accu-Vote TSX, Accu-Vote TSR6, Edge, eSlate, iVotronic, Patriot and AVC Advantage.

VITA began the security assessment in August 2017. Given the compressed timeframe with the upcoming November general election, VITA expedited the assessment of the voting systems and provided ELECT with a preliminary report. The report found that "each device analyzed exhibited material risks to the integrity or availability of the election process." VITA's initial findings concluded:

> "In each of the systems the potential for loss of vote is significant as none of the machines appear to produce paper audit trails during the voting process."

In a Sept. 8, 2017 memo to the SBE, ELECT Commissioner Cortés said, "As VITA's report contains confidential information related to voting system security, and some of this equipment is currently used in other states, the department further recommends that VITA's report remain confidential."

Based on the VITA assessment, questions about the integrity of its voting machines and the potential for cyberattacks, Virginia's three-member elections board voted unanimously to decertify DRE voting machines at a September 2017 board meeting and announced action to mitigate risk via a press release. Along with heightened national worries about foreign interference in the election process, concerns included:

- DREs did not maintain a paper record of individual votes
- Devices operated with a high level of risk
- Testing proved that the vulnerabilities can allow a malicious party to compromise the integrity of voting data

Questions were raised by stakeholders, including localities and advocacy groups, about an unfunded mandate for the purchase of new voting equipment. For example, the Virginia Association of Counties submitted an Aug. 30, 2017, letter to SBE regarding fiscal implications. Additional questions emerged about staff training and troubleshooting for new machines.

The concerns regarding the voting machines in 2017 were not the first voiced in Virginia. In response to prior voting irregularities reported during the November 2014 general election, Gov. Terry McAuliffe called for an investigation into Virginia's voting machines. Shortly thereafter, SBE unanimously voted to approve Commissioner Cortés proposal to conduct a comprehensive review of Virginia's voting devices.

ELECT issued a press release and report on April 1, 2015, and concluded after a Joint Committee to Study the Certification, Performance and Deployment of Voting Equipment that significant issues, including security concerns about the use of wireless communications were linked to the voting machines.

In a 2015 request from ELECT, VITA tested the Advanced Voting Systems WINVote devices and outlined significant security concerns in an April 14, 2015 report, Security Assessment of WinVote Voting Equipment for Department of Elections. ELECT followed the recommendations to decertify the DRE voting machines.

McAuliffe proposed $28 million in his 2014 budget to help local jurisdictions replace voting machines. While resources were earmarked to assist localities with replacement of voting machines, the General Assembly cut the funding from the state budget. As a result of prior IT security vulnerabilities with voting machines, legislation was passed in 2016 earmarking a July 1, 2020, deadline for localities to phase out DREs.

In May 2018, the Washington Post reported about similar voting machine challenges in Georgia. While lawmakers and others are requesting further inquiry about the systems, a nonprofit group and citizens are suing the state to end using electronic voting machines and switch to paper ballots instead. Virginia's swift action was cited.

In 2017, VITA assessed the DRE voting machines provided by ELECT and concluded that those machines operated with a high level of risk for Virginia's election process. VITA tested physical, network, operating systems and vote tally processes to assess for security vulnerabilities.

As a result, decertification of the devices for 22 localities was recommended. Once data and IT system analysis was concluded, support recommendations were provided for localities.

A concern raised by local leaders was the potential fiscal constraint associated with new voting machines. Several leaders sent correspondence to SBE about the additional expense for new systems. ELECT assisted some with payment arrangements and others rented devices. Specifically, five of the 22 localities with the decertified voting machines opted to purchase new equipment and the remaining seventeen rented voting devices. To assist those local leaders, ELECT worked with four certified voting machine vendors to ensure that the proper equipment was accessible and that there were various purchase options.

VITA utilizes the NIST cybersecurity framework and has robust cybersecurity standards and policies based on NIST guidelines. Both enterprise and MS-ISAC security sensors within Virginia's network provide alerts from federal sources on potential threats that could target the elect infrastructure or processes. Additionally, VITA conducted regular penetration testing using both internal and external resources. The Department of Homeland Security (DHS), the Virginia

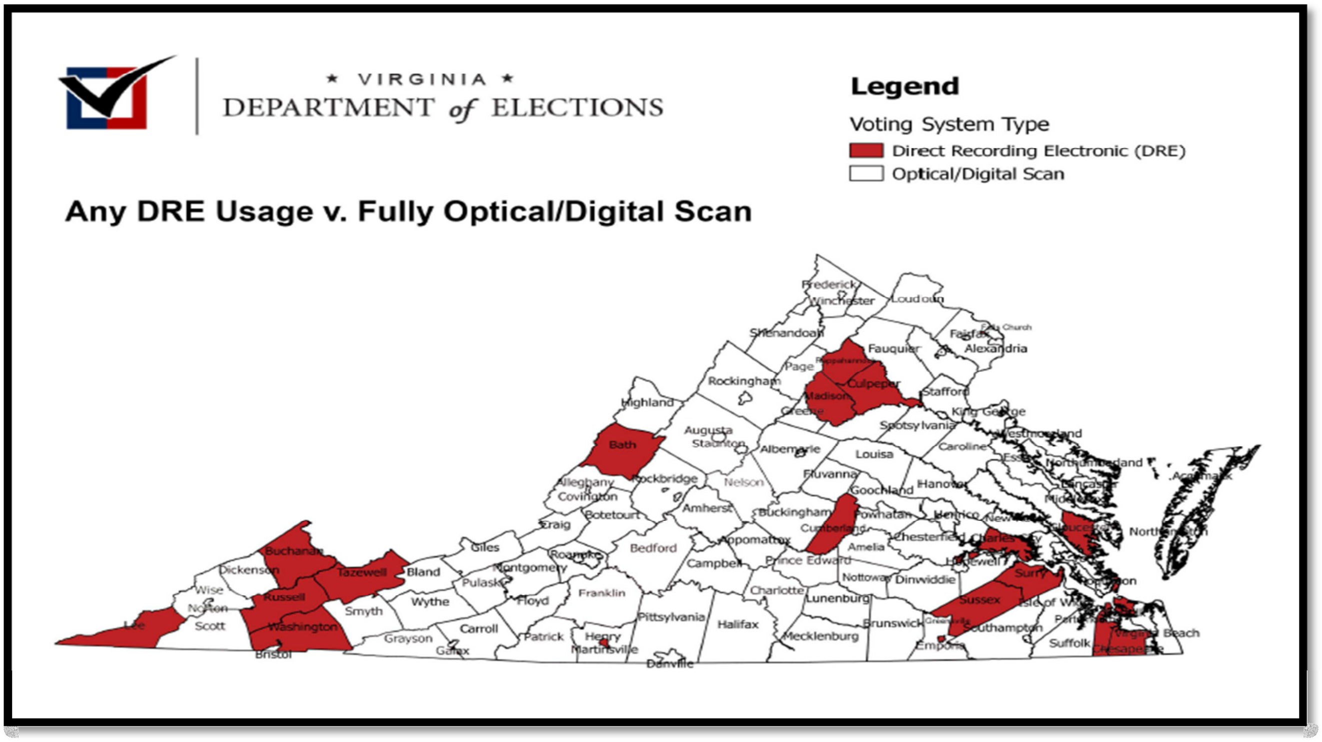
National Guard, and private industry were engaged for this testing. DHS penetration testing concluded in March 2018.

Significance

The decertification project protected commonwealth voting systems and information assets from misuse and damage. Safety mechanisms and precautionary measures were implemented to ensure the integrity of voting and that voting technology remained protected and accessible for Virginia's citizens.

This project aligned with NASCIO top 10 strategies and solutions, including security and risk management. It also ties in with the governor's priorities supporting IT initiatives and cybersecurity. The initiative supported two of VITA's strategic priorities including cybersecurity endeavors to protect the commonwealth and maintaining IT services. Furthermore, an annual strategy to provide cost-effective IT services that meet commonwealth standards was met through VITA providing ELECT with IT assessments for the DREs instead of contracting a private company.

As a result of the decertification initiative, the integrity of the commonwealth's voting system was maintained in the November General Election. This was a positive impact for citizens, state and local systems and IT infrastructure essential to protecting the democratic process in the commonwealth.



Source: September 9, 2017 Election Board Meeting Minutes. Elections.virginia.gov

Impact

Several benefits resulted from the decertification of the DRE voting machines. The DRE voting machine decertification affected localities serving 140 of the state's 2,439 voting precincts, or about 190,000 of Virginia's five million active voters. Stakeholders included citizens of the commonwealth, local government entities, advocacy groups, those seeking public office, VITA, ELECT and the SBE, among others, and aligned ELECT and SBE protocols with cybersecurity priorities and had direct benefits. These included:

1. Protection of Virginia's citizens by ensuring an accurate vote
2. Reinforcing ELECT protocols and future practices
3. Avoiding systemic challenges or voting irregularities
4. Proactively assessing IT data and risk
5. Negotiating payment arrangements or leasing options with vendors
6. Supporting and engaging localities to secure new voting equipment
7. Involving VITA in voting fraud prevention in the ISAC program and with DHS
8. Training, in collaboration with vendors, staff on new voting machine devices

By the November 2017 election, all impacted localities had secured alternative optical scan models. The most direct benefit was for citizens of the commonwealth. Above all, decertification protected voters from potential fraud. Affected voters were generally from lower socio-economic rural and urban areas and the state's efforts ensured they were heard. Also, Virginia was in compliance with best practices mandating that all voting systems were tested with Election Assistance Commission (EAC) Voluntary Voting System Guidelines.

Through ELECT's support, local government fiscal considerations were addressed. While there were financial and administrative burdens for many localities, new or rented machines were acquired in time for the November General Election.

VITA and ELECT worked in tandem to address the potential voting system threats. ELECT readily engaged the VITA commonwealth security and risk management staff to build on prior IT projects for ELECT and initiatives regarding voting equipment including the 2015 WinVote decertification and poll book analysis.

In a September 2017 press release, Elections Commissioner Cortés said, "The ability to meaningfully participate in our democracy is one of the most important rights that we have as citizens, and the Department of Elections is dedicated to maintaining voters' confidence in the democratic process."

In line with ELECT's priorities, Commissioner Cortés recommended additional security measures to protect the integrity of citizen votes. Included was a request for VITA to conduct an IT system analysis and risk assessment. Furthermore, he shared how significant the project collaboration was in a very short 59-day timeframe prior to the November election. On Nov. 29, 2017, Cortés provided testimony before the Congressional Committee on Oversight and Government Reform pointing out several cybersecurity goals that ELECT achieved. Specifically, he noted that ELECT leveraged technology to improve the voting experience for Virginia's citizens and improved accountability through more diligent security measures. Commissioner Cortés shared:

> "In essence, the decertifications have gone smoothly because of the teamwork between state and local officials, national organizations, state organizations, voting equipment vendors and the veritable army of officers of election who assist with administering our elections … Verified Voting also served as a resource and provided the department and VITA, under exceptionally tight timelines, with helpful information about the equipment's vulnerabilities."

Additionally, the VITA DRE voting machine assessment was conducted at a significant cost savings for ELECT and the taxpayers of the commonwealth. Given that VITA IT services are readily available for commonwealth agencies, specific duties executed by VITA's team were covered for the project rather than becoming an outside expense. Specifically, VITA leveraged internal resources from security architecture, incident response and risk management to perform the testing and assessment of the voting systems and pollbook solutions. These resources constituted more than 50 years of information security experience from combined management, risk and technical expertise. VITA personnel involved in the assessments hold a wide range of security and technical accreditation, including graduate degrees in information security, and cloud security, Certified Information Systems Security Professional (CISSP) and SANS certifications.

VITA's recommended decertification of the voting machines in an initial report was an opportunity for ELECT to further engage IT system analysis of pollbooks and other IT infrastructure to reinforce accountability and prevent cyberattacks. Removal of the devices throughout the commonwealth mitigated further risk and prompted proactive IT systems review.

To further protect the commonwealth, VITA and six other states participated in the ISAC Pilot for Election Infrastructure program co-sponsored by DHS and Multi-State Information Sharing and Analysis Center (MS-ISAC). Discussions revolved around malicious internet protocols (IPs) and domains, vulnerabilities, threats, potential compromises, incidents, patch advisories, intelligence products and election-specific cyber alerts.

The Virginia collaboration between VITA and ELECT led to voting machine decertification that maintained the integrity of Virginia's voting systems. The VITA assessment highlighted vulnerabilities for the commonwealth that protected the commonwealth. Potential hackers and other cyber attackers were denied entry through skills protection of Virginia's voting systems.