Election Security: Fortifying Election Localities with Policy and Planning

A Technical Report Submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Harshal Nallapareddy

Fall 2024

Technical Project Team Members

Tyler Burkhardt

Jeremy Wint

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Jack W. Davidson, Department of Computer Science

Election Security:
Fortifying Election Localities with Policy and Planning

CS4991 Capstone Report, 2024

Harshal Nallapareddy
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
cze6kb@virginia.edu

ABSTRACT
Election localities in Virginia must comply with a set of state-certified standards dubbed Locality Election Security Standards (LESS); however, the lack of resources makes compliance difficult for many rural Virginia localities. As part of the Virginia Cyber Navigator Internship Program, our group collaborated to assess, improve and maintain Amelia County's LESS compliance. Our work began with evaluating the current state of compliance and creating a plan to incrementally improve compliance. Over the summer, we wrote and updated Incident Response Plan, Risk Assessment, Business Impact Analysis, and guides for installing security and logging software on office computers. As a result, Amelia County's baseline LESS compliance increased from 74% to 87.5%. We saw similar improvements in preferred and platinum requirements, and compliance is projected to increase to 97.1% upon implementing the remaining guides. The next steps to reach 100% compliance include installing physical monitoring of secure areas, establishing access control and audit functions, and performing penetration testing.

1. INTRODUCTION

In the 2000 U.S. presidential election (Bush v. Gore), thousands of voters in Palm Beach County, Florida, inadvertently cast ballots for the wrong candidate due to the confusing nature of the butterfly ballot, resulting in recounts and court battles ultimately shaping the winner of one of the most disputed elections in American history. This incident underscored the critical role of election security and integrity, highlighting vulnerabilities not just in voting equipment but in the overall infrastructure that supports free and fair elections.

In 2024, election security remains a pressing concern for the nation, and while technology has improved the electoral process, rural localities with fewer resources continue to fall behind. Ensuring compliance with election security standards like LESS is crucial in preventing election vulnerability that could undermine public trust. This issue is especially prevalent in modern times, given the potential for cyber-attacks interfering with election infrastructure prior to 2024 presidential elections.

Ensuring that all localities meet stringent security standards is more vital than ever. Our work in Amelia County, conducted through the Virginia Cyber Navigator Internship Program, addresses the challenges rural election localities face with meeting LESS compliance. By improving their security protocols and updating key documents, we aimed to enhance the integrity of Amelia County's electoral process in preparation for future elections.

2. RELATED WORKS

Election security has become a focal point in discussions about national security. Experts like Manpearl (2018) discussed the fact that the controversial 2000 presidential election compelled Congress to enact the Help America Vote Act (HAVA) to reform the election process. HAVA required states to create "computerized voter registrations lists" that allowed Americans to register to vote online. Congress also required states to "provide adequate technological security measures to prevent unauthorized access to the computerized lists." However, the Election Assistance Commission (EAC) did not develop technological standards for protecting these systems, leading to third-party vendors developing and maintaining subpar systems. Virginia's LESS guidelines are a direct response to the lack of national guidelines, and our group's work in Amelia County specifically addressed these guidelines to build a strong technological foundation.

The majority of our group's work was preparing contingency planning for election emergencies. Scenarios such as natural disasters, technological failure, and human error necessitate election localities to be prepared and vigilant to recover. Brown, et. al. (2020) cites the 2001 terrorist attacks, Russian cyber-attacks, several hurricanes, and the COVID-19 pandemic as disruptions to the critical election infrastructure and emphasizes that "operational contingency planning" is necessary to ensure seamless responses to such events. This type of planning is pertinent in light of recent events such as the July 2024 CrowdStrike outage that rendered computer systems around the world inoperable. Ensuring that Amelia County has robust contingency plans in place was essential in maintaining election integrity.

3. PROJECT DESIGN

Before pursuing any planning or implementation, the group conducted an initial evaluation to assess the current state of Amelia County's compliance with LESS. This assessment provided a baseline understanding of the locality's existing security protocols and identified key areas that needed enhancement. At the time of evaluation, Amelia County reported an approximate 70% compliance; however, upon further inspection, it was estimated to be closer to 50%. Our evaluation revealed five major security gaps: secure communication, data/system backups, incident response, inventory management and miscellaneous security or training measures. Based on this evaluation, the group developed a targeted approach to significantly improve the security standing in each of these areas.

3.1 Encrypted Email Communication

The first critical gap in security was the lack of secure communication protocols between locality officials and third parties. The absence of encryption meant sensitive election-related information could be potentially intercepted. To address this, adopting encrypted email solutions was recommended to ensure all communications between locality officials and external parties were secure. A few characteristics of a viable encrypted email solution were ease of integration into the county's existing email infrastructure and proper training/documentation of its use.

3.2 Data Backups and Recovery

The second key area of focus was a reliable backup system is essential for protecting election data against loss, corruption, or tampering. During the evaluation, the group discovered that Amelia County's backup processes were irregular and lacked automated features. To improve this, we designed and implemented a comprehensive backup strategy that includes regular, automated backups of critical election data. We also ensured that backup data is securely stored offsite to protect against local hardware failures or natural disasters, enhancing both

the reliability and recovery capability of the system.

3.3 Incident Response Planning

The third area was to develop a robust incident response plan, as the existing one lacked depth and clarity. In election emergencies, such as cyber-attacks, system failures, or physical breaches, quick and effective responses are crucial. We collaborated with county officials to create a detailed incident response plan that outlines clear steps to follow in various emergency scenarios. This included training local officials on how to respond to different types of incidents and performing simulated drills to ensure readiness.

3.4 Inventory Management

Maintaining an accurate and up-to-date inventory of election equipment and software is vital for effective security management. Our evaluation found that Amelia County's inventory records were outdated and inconsistent. We developed a systematic inventory management process that not only tracks all hardware and software but also monitors their lifecycle and updates. This improvement ensures that election officials have a comprehensive understanding of their assets and can better manage security risks associated with outdated or unsupported equipment.

3.5 Miscellaneous Security Enhancements

Finally, we addressed several miscellaneous security concerns that did not fall under the previous categories. This included role-based training, media destruction policies, Business Impact Analysis, password management policies, and other odd tasks. These miscellaneous improvements helped close smaller but significant gaps in the county's baseline, preferred, and platinum security posture, contributing to the substantial improvement in LESS compliance.

4. RESULTS

The majority of the work done was in the form of policy documents and guides created or updated by the group. These deliverables fall into one or more of the five categories from the previous section, and each serves to fulfill one or more of the specifications listed in LESS. However, the encrypted email category remained unfulfilled due to the locality's budget limitations that prevent the office from upgrading the Microsoft 365 license to the Enterprise tier that includes encrypted email. The second category, data backups and recovery, several documents such as the Data Classification Policy, Guide to Backups for Windows 10 Devices, and Guide to Recovery for Windows 10 Devices outline critical processes for implementing backup strategies where the guides lay out specific instructions to set up the required systems.

The third category, incident response planning, consisted of several training and policy documents that focus on preventative measures and post-incident procedures. Cybersecurity Incident Training documents focus on preparing personnel on how to response or behave during security breaches. Incident Response Plan and Incident Reporting Procedure offer frameworks for responding to security breaches as they are happening, and Post-Incident Response Interview and Remediation Plan help retrospectively address the issues that arose during the incident and how to prevent them in future breaches. The fourth category, inventory management, consisted of three main deliverables: Hardware Inventory, Software Inventory, and Network Diagram. The Hardware and Software Inventory documents provide a detailed record of all physical equipment present in the office as well as the computer systems used by the election locality officials. The Network Diagram illustrates the connections between systems to visualize the physical and virtual

infrastructure; however, many parts of the network diagram require a further analysis by an IT specialist, since much of the ethernet wiring is hidden within the walls of the office. Finally, there are several documents and guides that cover security measures outside of the previous categories. Specifically, documents such as Media Protection and Destruction Policies outline safe storage and disposal and sensitive materials while Access Records keep track of who has access or has access to secure areas and information systems. As a result of the guides and policy documents, the final LESS compliance for Amelia County progressed from 74.0% to 87.5% on the baseline level, 70.8% to 87.6% on the preferred level, and 67.5% to 84.4% on the platinum level.

5. CONCLUSION

By addressing the five major security gaps, our project design has laid the groundwork for significant improvements in Amelia County's compliance with LESS. Equipping the local personnel with resources and guidelines training, incident response, secure data management and other security targets not only brought the county closer to achieving full compliance but also strengthened its ability to prevent potential threats, ensuring a more secure and resilient election infrastructure. Through the experience, I gained a deeper understanding of cybersecurity measures and the complexities of protecting election infrastructure. I also learned skills such as writing detailed, actionable technical documents and assessing the security posture of critical systems.

6. FUTURE WORK

In order for Amelia County to reach 100% LESS compliance, there are three main security goals. The first is equipping secure areas of the office space with physical monitoring systems through surveillance cameras and card readers to monitor access and enhance security. The second goal is to access control and audit functions to reach a strong separation of powers between the office's local personnel. However, given that there are only two employees in the office, it is difficult to maintain that separation of power, since the deputy registrar needs to have access to all resources and systems in the absence of the registrar. The third goal is penetration testing conducted by a qualified third party to simulate a cybersecurity attack and identify any vulnerabilities.

7. ACKNOWLEDGMENTS

I would like to thank my team members Jeremy Wint and Tyler Burkhardt for their collaboration on this project, and I also wish to extend my gratitude to Professor Jack Davidson, Professor Deborah Johnson, Professor Angela Orebaugh, and all the professors involved in the Cyber Navigator Internship Program for their support and guidance throughout project. I would like to recognize the Amelia County registrar Deborah Hathorn for her cooperation.

REFERENCES

Manpearl, E. (2018). Securing US election systems: Designating US election systems as critical infrastructure and instituting election security reforms. *BUJ Sci. & Tech. L.*, *24*, 168.

Brown, M., Forson, L., Hale, K., Smith, R., & Williamson, R. D. (2020). Capacity to address natural and man-made vulnerabilities: the administrative structure of US election system security. *Election Law Journal: Rules, Politics, and Policy*, *19*(2), 180-199.