State of Delaware

Department of Elections

Department of Technology and Information

Department of Transportation/Division of Motor Vehicles

Delaware Criminal Justice Information System

Election System Migration
Category: Cross-Boundary Collaboration & Partnerships
Project Initiated: September, 2018
Project Completed: November, 2019

Contact:
James Collins, State CIO
james.collins@delaware.gov
302-739-9500

Executive Summary

Over the past several years, there has been an increasing number of reports regarding cyber-attack breaches of election systems nationwide. Due to the heightened awareness regarding these attacks, leadership from the Department of Elections (Elections) and the Department of Technology and Information (DTI) proactively formed a team to exclusively work on assessing Delaware's election system in order to identify and correct any vulnerable areas and modernize the system. The team assessed the election system in July and November 2017, providing DTI and Elections leadership with a list of the security vulnerabilities that were discovered. With this project, initiated in 2018, the State of Delaware has successfully modernized the Statewide Election System in preparations for the 2020 General Election. The modernization project included both the Voting Machines and Voter Registration software. The enhancements include: implementing new voting machines, which are certified by the U.S. Election Assistance Commission; establishing a paper record of each electronic ballot cast, and enhanced security on all network communications.

All of the modernization enhancements and implementation of a federally certified voter tabulation system were completed in time for a successful school board election in May 2019. Voter registration software was fully deployed in November 2019, well before the 2020 election year cycle began. This project ensures the protection and integrity of Delaware's electoral process and voter data, enhances scalability, and increases voter confidence.

Exemplar

One of DTI's strategic goals is delivering Reliable, Secure, and Resilient Services. DTI oversees Executive Order 55, Establishment of the Delaware Cyber Security Council, which focuses on developing best practices to mitigate cyber security risks and improve the overall security posture of the State. The iVote project directly relates to Executive Order 55 objectives centered on cyber security protections. Due to heightened awareness regarding the increasing prevalence of election systems cybersecurity attacks and data breaches, leadership from the Department of Elections (Elections) and the Department of Technology and Information (DTI) proactively formed a team to exclusively work on assessing Delaware's election system. The goal was to identify and correct any vulnerable areas to prohibit malicious users from gaining access to secure Delaware voter information. The benefits of this project were to secure Delaware's election system and processes, thus providing integrity in the process and the confidence of our citizens. Election systems were also designated critical infrastructure by the federal government.

Concept

Department of Elections and DTI leadership and management were engaged during a 2017 assessment with the anticipation that some remediation work would need to be completed. Support was obtained by outlining the vulnerabilities, risks, and impacts. Given the cross-agency touches noted below, it was imperative for Elections to form a team comprised of stakeholders from each agency. The Department of Elections was mandated by legislation to implement system(s) that are federally certified by the U.S. Election Assistance Commission. Title 15 § 5001A (c).

 The Election System Migration team was created to move the elections system off the DTI Mainframe, implement a federally certified tabulation system, create a paper record of ballots cast, and to integrate a Software as a Service Voter Registration System with several state agencies. IT processes that are necessary for a fully functioning election system includes results transmission, storage of election data collected from the voting locations, and logging of all transactions and activities throughout the election system. The team was extremely dedicated and aware that the work they were doing was not only important to DTI, Elections and the General Assembly, but also to Delaware citizens. Each team member took personal ownership in delivering solutions that modernize and harden critical Elections systems.

In order to properly convey the impact and risk of cyber security vulnerabilities identified in the 2017 assessment, the team had to translate information from technical to non-technical terms for the senior leadership of DTI and Elections. The team proactively evaluated major components of Delaware's election system using a combination of security scanning tools and manual reviews of software, networks, and processes to determine areas of vulnerability. Prioritization of these vulnerabilities was made jointly by Elections and DTI as to the areas where significant enhancements could be made within the allotted timeframe. In order to provide Delaware's citizens with a secure system and confidence regarding the safeguarding of their information, this project was made a top-priority for both agencies

DTI's Application Delivery team was the initial sponsor/champion. They began the election system assessment in July 2017.   DTI and Elections leadership and management were engaged during the assessment with the anticipation that some remediation work would need to be completed.

Support was obtained by outlining the vulnerabilities, risks, and impacts. The team communicated continuously with each other on a daily basis through formal meetings and informal emails and discussions. The members had touch points with the customer on a bi-weekly basis. The team communicated with leadership through weekly written status updates and scheduled monthly meetings. Detailed descriptions of challenges and technical fixes to those challenges helped frame the reason why changes were needed. Demonstrations to the Elections personnel after each sprint kept all stakeholders updated. System testing scripts, utilizing a template for consistency, assisted testers in understanding the desired functions or output of a software component. Department of Elections handled communication with any other interested parties, that were not project stakeholders. DTI leadership provided feedback to the project team on a monthly basis and when requested. DTI leadership also provided direction when technical team members could not reach consensus on the best course of action for various cyber security issues and proposed fixes. The Chief Information Officer acted as a liaison with the Elections Commissioner.

The team provided a list of security vulnerabilities to DTI and Elections leadership in November 2017. The list categorized the security vulnerabilities by risk (critical, high, medium and low), specific election processes (election results tabulation, voter registration, counting of absentee ballots, and acceptance of provisional votes), supporting technical discipline (network layer, application layer) and estimated remediation time for each identified vulnerability category. The vulnerabilities were prioritized jointly by Elections and DTI. The team officially began system remediation efforts in May 2018 with a project to enhance the iVote application, completed in August 2018.

This subsequent project, to migrate from mainframe to cloud, began in September, 2018. The project was comprised of two phases, each with their own implementation date.

- The Tabulation portion of the project implemented beginning in May of 2019. The Tabulation system includes: Voting Machines, Paper Ballot scanners, Poll Books, etc.

- The Voter Registration portion of the project implemented beginning in November of 2019. The Voter Registration system includes: managing registered voters, absentees, reporting, printing of Polling Place Cards, tracking historical residency requirements, etc.

The goals of this project were lofty and complicated by the fact that Delaware is the pioneer in real-time integration between Voter Registration and Delaware's Department of Transportation's Division of Motor Vehicles (DelDOT/DMV). Given all of Elections past successes, the team had to ensure that real-time integration was maintained or enhanced with our State of Delaware partner agencies.

Achieving the goal of moving off the DTI mainframe was a significant effort because it required Elections to rethink real-time agency integration and security concerns in moving to the Cloud. Each of these factors presented challenges since real-time integration with other state agencies was required and communication with the vendor had to be secure. To ensure success, Elections' staff from the department and all three counties formed a multi-agency team with DTI, DelDOT/DMV, Delaware Criminal Justice Information System (DELJIS) and the Department of Correction (DOC) to encourage collaboration and coordination between agencies.

Significance

New cyber security threats are detected daily; addressing vulnerability to these threats is an ongoing task for all IT professionals. The Elections systems are used not only for federal elections but also for state, local, and school board elections throughout the year. Elections systems continue to be in use

and monitored by DTI security systems and personnel in real time to determine if and/or when a malicious attack is attempted. During the 2017 Elections evaluation, security vulnerabilities of various levels were discovered and documented. Elections and DTI leadership recognized the importance of implementing new and improved security controls to enhance services delivered to our citizens. By evaluating, purchasing, and implementing security scanning toolsets for applications, the expediency and quality of the evaluation vastly improved. This project, which added federally compliant

The primary stakeholders affected by this project were Elections, DTI, DelDOT and DELJIS, and, more importantly, every Delaware citizen registered to vote. The benefits include increased security of citizen voter information, successful transmission of election results, modernized and secure software, and enhanced auditing practices. Each of these system improvements leads to less entry points for cyber criminals, better methods to discover attempted attacks, and higher integrity of (and higher citizen confidence in) Delaware's election results.

Impact

The impetus to implement the Election System was driven by the desire to modernize the voting machines and to move the Voter Registration System off the DTI Mainframe. As per Delaware Code, the new voting machines are certified by the U.S. Election Assistance Commission (EAC)and now include a paper record of each ballot cast. Additionally, the new voter registration system has been moved to a cloud provider which eases the burden of hosting and support by State of Delaware's resources. Both systems, the Tabulation System and the Voter Registration System, have benefited from increased security measures that reduce the risk of a system compromise, thus increasing the overall security of Delaware's Election System. Finally, the new voting machines now create a paper record of every ballot cast. This provides a visual confirmation to Delaware voters that their votes are being cast correctly, enhancing citizen confidence in election outcomes.

Moving Elections off the DTI mainframe reduced the amount of in-house technical resources needed. A vendor is now tasked with ensuring the system infrastructure and applications are secure, updated, and performing well. The stakeholders measured the enhanced election system against the priority list of enhancements. To date no unauthorized elections system access reports have been registered. Enhanced auditing monitored the system in real time to ensure integrity of local and school elections until this migration to a new voting system could be completed. Delaware Cyber and Application Security Standards are the minimum that should be applied to application coding practices in State agencies; however, agency leadership can change their approach to be more stringent depending on the criticality of their applications and other federal regulatory requirements. The scanning toolsets follow the same principle, where minimum scanning algorithms are applied to application code, but custom algorithms can be added to the minimum algorithm to address unique cyber protections within each agency based on their technology assets, federal requirements and services provided to the public.

Several security attributes were addressed with the implementation of the new Election Management System. Physical Security, data encryption, data monitoring and network segmentation have been used to ensure the Election Management System remains secure and meets or exceeds state standards and industry standards. The ESM team acknowledged that security was Delaware's number one priority and the new system has increased security internally

and externally. Internally, the tabulation system (the system used to receive ballots) is using its own VLAN to communicate across the state. Externally, the Voter Registration System is using enhanced security protocols to protect Personally Identifiable Information (PII) when communicating with our cloud-based vendor.

The new Voter Registration System had to be integrated with the Delaware Criminal Justice Information System (DELJIS) to provide felon checking capabilities. Historically, this felon check interface involved file clerks at the Department of Correction (DOC) to perform manual research for some of the voter registration applications received. The new felon check process automates much of this manual research by using Criminal Justice Information System (CJIS) data from DOC and DELJIS data. Essentially, by combining the data from DOC and DELJIS, the system can determine if an applicant is a felon and if they have completed all their sentencing and probation, thus automating much of the research performed by file clerks in the past.

The DMV assists with voter registration by promoting access to elections via their Over-the-Counter process, MyDMV Online, and the Kiosks located at each of the DMV locations. All of these DMV resources access the new Election Management System in real-time, so it was imperative for Elections to provide enhanced security and a workflow that did not impact DMV wait times, identified by stakeholders as important.

This project accomplished several areas of efficiency. First, the process allowed Elections leadership to work closely with three county teams to work together to assure that the new system could accommodate differences in day-to-day processes among the offices. Second, by moving to a cloud provider the Department of Elections was able to eliminate the use of the DTI mainframe and reduce the number of servers managed by state resources. Additionally, the new felon check process has the capability to reduce the amount of research work performed by the Department of corrections records staff. The team's successful outcome is measured by the functionality and performance of a system that is heavily and consistently utilized by multiple constituencies. The team's work provides a more user-friendly, intuitive and, ultimately, more functional interface for the various constituents of Delaware elections. By all measures, the project has been successful as implemented. Results will be ongoing and sustained by regular system maintenance and upgrades/updates, as available—some based on user input and feedback.