Report to the Texas Legislature on Election Cybersecurity Preparedness

November 30, 2018

Abstract

The Office of the Texas Secretary of State ("SOS" or "Our Office") conducted a study regarding cyber attacks on election infrastructure and submitted two reports to the standing committees of the legislature with jurisdiction over election procedures: A summary report for the public and a general compilation report for legislators. This is the summary report for the public.

Keith Ingram

KIngram@sos.texas.gov

SUMMARY REPORT

Election infrastructure in Texas can be divided into four broad categories: (1) the voting equipment itself and the associated computers that program the ballots and tabulate the results; (2) the statewide voter electronic voter registration database; (3) the candidate management, election night reporting, and canvass systems maintained by SOS; and (4) the public-facing websites of SOS and the counties. Our Office is not aware of any successful cyber attack on any of these infrastructure components.

In conducting this study, Our Office visited several counties in the central Texas area. Our Office included a mixture of small, medium, and large counties with a variety of different voting systems. Our goal during these visits was to assess whether or not the counties were following security procedures required by law and as advised by Our Office. The SOS staff also visited with the largest voting system vendors operating in Texas about the security of their legacy and current voting systems including supply chain security. Finally, Our Office had extensive discussions with the voter registration database vendor regarding their security measures and back up procedures.

During the SOS staff visits with counties, Our Office learned that election officials in every county visited were familiar with and following these security procedures. The SOS has a fairly high degree of confidence that the voting equipment that is owned and kept by the counties would be difficult for an adversary to compromise. In addition, Our Office believes that if the procedures prescribed under current Texas law are followed, any potential compromise would be detected and mitigated as to allow for a successful election to be conducted.

Our Office believes the statewide electronic voter registration database is as secure as currently possible, and there has been no evidence of penetration, unauthorized access, or manipulation of voter data or records contained in the database. Our Office used a small part of the recently appropriated federal funds to increase our security posture. Once the federal funds are expended, some continuing obligation on the part of state government will be necessary to continue to maintain these efforts.

It is vitally important that all Texas counties take the state up on its offer to assess their election systems using the Help America Vote Act ("HAVA") money recently appropriated. Given the relatively high level of resources available to larger Texas counties, it is believed that their data to be reasonably secure. At the same time, Our Office must ensure that counties with fewer resources can receive the same security assessments and take appropriate measures to mitigate any risks that may be identified.

A final recommendation regarding security of the voter registration database is to pass legislation enabling the SOS to require cyber training for all of the users of its systems. Our Office has made "Securing the Human" training available to county users at no cost. However, Our Office has no ability to require them to take the courses, only the ability to encourage them take advantage of this free and useful resource.

The SOS has implemented multi-factor authentication on the candidate management, election night returns, and canvass pieces of the election infrastructure. These programs are segmented from one

another in different systems, which creates both security and maintainability challenges. The goal of Our Office is to upgrade to one sustainable, secure end-to-end system – from candidate filing through the canvass of the general election, and Our Office is currently exploring that possibility.

It is important to remember that, contrary to the news reports out of the DEFCON Conference this year, an 11 year old has not demonstrated the ability to "hack an election." There is a large and important difference between the reporting of unofficial election results on election night and the actual election results. If a malicious actor were to manipulate posted vote totals or if there were a DDOS attack on the reporting website, the actual results would not be affected.

Our Office has contingency plans to record accurate vote totals and display them to media for reporting to the public in the event of a disruption in our election night reporting system. Our Office believes the elections system in the State of Texas to be extremely resilient, due in no small part to the hard work and dedication of local election officials in maintaining proper security protocols. Year after year, Our Office and local officials routinely demonstrate the ability to work together to facilitate a fair and legal voting process to continue unabated despite occasional technological challenges.

The public-facing websites maintained by Our Office and those of the counties do not contain any confidential information or any votes. However, it is important that these websites remain available and that they provide accurate election information to the voters and to the general public throughout the process. The Web Services vendor has state of the art security. Counties' public-facing websites are maintained and secured by the counties.

In March of 2018, the U.S. Congress appropriated the last $380 million authorized by HAVA, of which Texas received approximately $23.3 million. In releasing these funds, Congress emphasized that states should emphasize strengthening election security when utilizing these funds. Texas plans to use approximately 2 million of these dollars to upgrade security of TEAM and to institute a secure end-to-end candidate filing, election night returns, and canvass system.

The remainder of the money will be spent on enhancing the security of county election systems. Our Office is making available to all 254 counties in Texas a customized and comprehensive Election Security Assessment which will assess various components of county election security, including both physical security was well as cyber security. These services are being procured as Managed Security Services covered under the Interagency Contract between DIR and Our Office. Remaining funds can be used to subsidize priority upgrades to county election infrastructure, if needed.

In summary, Our Office understands completely that election infrastructure security is an ongoing and never-finished race. The federal money recently appropriated will aid us and the counties tremendously as Our Office engages in protecting Texas elections from those who would seek to do harm to us and to our most important civic institution. Our Office is confident that Texas voters can trust the election systems, and Our Office is working constantly to ensure that they can continue to have this confidence in the future.

The recommendations made are as follows:

- Personnel and travel budget to provide on-site assistance and advice to county election officials regarding security measures and voter registration list maintenance procedures.
- Enabling SOS to require that users of its systems complete basic security training courses.
- Implementing additional end point security.
- Requiring counties to report cyber security breaches to Our Office when they occur so that we can assist them in mitigating the damage as well as remediation.
- Requiring users of the statewide voter registration database to undergo annual cyber hygiene training provided by the state.