STATE OF RHODE ISLAND AND PROVIDENCE PLANTATIONS

BOARD OF ELECTIONS
50 Branch Avenue
Providence, RI 02904
(401) 222-2345
www.elections.ri.gov

August 9, 2019

FOR IMMEDIATE RELEASE:

Board of Elections addresses cybersecurity concerns about voting system

Providence, RI: Recent articles in online news publications have raised cybersecurity concerns regarding Rhode Island's voting system and use of modems to transmit unofficial election results on Election Night. Many of the issues raised in the article are inaccurate or outdated. The following Frequently Asked Questions has been created to address the issues raised in the article. An additional Election Systems and Software (ES&S) FAQ regarding the security of transmitting unofficial election results has also been attached to this release.

RI Voting System Cybersecurity - Frequently Asked Questions (FAQ)

Is Rhode Island's voting system online?

No. A data communication server, which is separate from the Election Management System (EMS) where votes are tallied, is securely configured to receive only unofficial election results from each DS200 in each of the state's 461 polling places on Election Night. The DS200 encrypts the file containing the results using industry-standard encryption protocols and initiates an encrypted connection to the data communication server. Only the DS200 can initiate this connection, which is initiated as part of pollworker closing procedures. The connection lasts approximately 30 seconds. The article contains an inaccurate diagram labeled Rhode Island EVS 5.2.0.3/5.3.0.3, Rhode Island System Configuration". It is dated October 23, 2015 which is prior to the state purchasing the new voting system in 2016. The diagram was part of an initial proposal by ES&S and does not reflect the current voting system configuration.

Is the data communication server active year-round?

No. The data communication server is activated shortly before the polls close at 8 p.m. on Election Night. It is also active periodically during the few weeks leading up to an election for testing or training purposes. For training, a separate server is activated to simulate transmission during classes for pollworkers. At all other times, the data communication server is physically disconnected from the ISP connection. It has not

been connected or powered-on since November 7, 2018. Transmission of unofficial election results does not occur for local special elections.

Are official results transmitted through modems?

Absolutely not. The morning following the election, all 39 cities and towns, including New Shoreham (Block Island), must transport the encrypted USB drive from each precinct DS200 to the Board of Elections offices in Providence. These encrypted drives are physically loaded into our Election Management System (EMS) to generate official results. These results are compared to the transmitted results from Election Night to identify any potential discrepancies. There were no discrepancies found after the 2018 General Election after this comparison was completed. If an encrypted drive is ever compromised or damaged, the Board can still recount the paper ballots.

Why does the article say Rhode Island's system was found online?

This is unclear since the article does not indicate when they conducted their scans and neither the author or the researchers contacted the Board of Elections for any information. It is possible that researchers were detecting a secure network that is necessary for the maintenance of the state's electronic pollbooks, which until August 2018 shared the same ISP connection as the data communication server, but nothing else. Maintenance of e-pollbooks occurs year-round for special elections and financial town meetings.

What has the Board of Elections done to secure the state's voting system?

In June 2017, the Board of Elections sought the assistance of the state Chief Cybersecurity Officer Mike Steinmetz to assist in convening state cybersecurity experts to analyze the state's voting system and identify any potential areas which could be improved from a security or best practices standpoint. Mr. Steinmetz assembled an informal working group consisting of experts from the state Department of Information Technology (DoIT); the Rhode Island National Guard Defensive Cyber Operations Element (DCO-E) , and the Rhode Island Fusion Center (an intelligence sharing collaborative between the RI State Police and several federal and state agencies); and RI Secretary of State. Over the course of 8 months, the group met regularly at the Board of Elections offices to gather information, assess the system, and determine any corrective action needed.

DoIT staff visited the Board of Elections facility several times to conduct a security assessment on both the voting system network configuration as well as physical security of the network facility. The RI National Guard's Defensive Cyber Operations Element (DCO-E) deployed staff to the Board of Elections facility to assess the network configuration for the voting system and e-pollbook systems. The DCO-E also conducted a field assessment of equipment at the polls during a special election conducted in Scituate in January 2018.

By June 2018, both DoIT and the RI National Guard's Defensive Cyber Operations Element had submitted their findings to the Board of Elections and found no major areas of concern with the current configuration or security measures implemented. Many of the recommendations involved best practices such as: how to establish sufficiently complex passwords; changing passwords each election; disconnecting the data communication server when not in use; changing IP addresses each election. All the recommendations were implemented.

In August 2018, to enhance security even further, the Board requested that Verizon initiate development of a Verizon (Zero Tunnel) Private Network. With the Verizon Private Network, neither the firewall nor the data communications server are connected to the internet. All transmissions stay on the Verizon Private Network and never connect to the public internet. Only Verizon Private Network certified devices are used in the private network architecture. Verizon Private Networks are specifically designed for high-security applications in critical infrastructure environments. This solution has been tested by federally accredited voting system test laboratories and proven in a number of recent implementations in other jurisdictions that use modems to transmit unofficial election results. Unfortunately, the Private Network was unable to be completed in time for the 2018 General Election. However, Verizon has since completed the private network and it is ready for implementation in 2020.

In late October 2018, prior to the General Election, the Board of Elections requested that DoIT conduct an audit of the firewall and data communication server portions of the voting system. These systems had been active periodically during the testing and training period prior to the November General Election and the Board wanted to ensure there had been no attempts to penetrate the system or that no anomalies existed. The audit found no unusual activity or anomalies within the logs of these devices while they were active.

Furthermore, critical security patches are regularly applied to the state's voting system, and the system is up-to-date with all security updates. These patches are only performed using a physical disk on-site by ES&S staff in coordination with state IT staff. Updated security patches were last made in January 2018 and July 2018. No security patches have been released since that time. The Board continues to monitor for the release of any new critical security updates necessary in the future.

Finally, prior to and during each election cycle, the Board works closely with DoIT to assess the configuration of the voting system to ensure all security measures on all components are fully implemented and best practices are being followed. This joint effort will continue throughout the 2020 election cycle to ensure robust security practices are being implemented effectively.

Was an IP address included in a publicly available document?

In 2017 a local cybersecurity expert contacted the Board of Elections with an interest in the security of the state's voting system. The Board met with this individual and provided him with all requested information that did not involve sensitive areas of the system. The individual issued a public records request for documents related to equipment-testing for several special elections and electronic logs for the DS200 voting machines used in the 2016 General Election. With an interest in providing information to the public and complying with public records laws, the staff reviewed the request with legal counsel, and it was determined the information was public record. However, a single instance of an IP address had been included in the logs which consisted of hundreds of thousands of lines of entries. It was quickly discovered and the IP address was immediately changed. As a security measure, the IP address is changed prior to every election.

Does the Board of Elections plan to use modems for unofficial election results during the 2020 election cycle?

In mid-2018, Election Systems & Software (ES&S) notified the Board of Elections that the modems currently installed in the DS200 would be obsolete by January 2020 because they utilize 3G technology, and the wireless network will only support 4G devices at that time. At a meeting on Aug. 6, the Board voted to continue the question of purchasing replacements modems until more research can be done on security of the devices and the jurisdictions in 11 other states that utilize ES&S modems for unofficial election results. ES&S indicates 33,741 modems are currently in use in these jurisdictions, and 12,169 have already upgraded to 4G Modems.

A decision on whether to deploy modems in 2020 will be made once the Board has acquired all of the information necessary to make an informed decision. Transmitting unofficial results securely on Election Night remains the fastest way of acquiring unofficial results on Election Night. The Board remains committed to continue working with our cybersecurity partners to address any security concerns before deciding to leverage this technology so that public confidence in the voting system is maintained.

MODEMING

As It Relates To Unofficial Results Transmission

Accuracy, security and reliability are the cornerstones of the ES&S development process for each voting system we manufacture and sell. From concept to construction, ES&S adheres to industry-leading standards and complies with rigorous testing schedules set forth by federal and state election agencies. Upholding and perpetuating the integrity of our nation's election process is our continuing mission as a company.

Where approved, certain ES&S systems support secure wireless network results transmission utilizing a Data Transmission Security bundle configured in the Electionware Configure module. The security bundle is loaded to the DS200 using USB media. The encrypted security bundle contains network access passwords to facilitate secure connection and authentication with the central reporting location. Only unofficial results are ever transmitted via modem. Official results are physically uploaded at the election office.

Additional security is achieved by signing the encrypted results bundle with a private key created by the DS200. The encrypted results bundle, in addition to the results, includes the signature file and DS200 created Public key used to verify the results bundle signature.

ES&S application software digitally signs every cast vote record and digitally signs the package of cast vote records captured by the tabulators.

Additionally, ES&S application software for the DS200 places a digital signature on all data sent to the tabulators on removable media — from the Election Management System (EMS) — and all data returned from the tabulators on removable media (to the EMS). The jurisdiction's election administrator assigns a unique account and password to all users of the EMS PCs

Modem capability is only activated when the polls are closed and communication is initiated to a designated host site for purposes of results transmission. Even when the modem is active the unit is not capable of establishing a connection that it did not initiate. Results are transmitted over a secure and encrypted connection.

Elections FAQ:

Frequently asked questions about transmission of unofficial election results.

In a some jurisdictions across the country, cellular modems are used to transmit unofficial results from polling places to election headquarters. These early, unofficial results help the news media report results quickly on election night. Final official results are physically uploaded at election headquarters prior to the final certification of elections.

Below are the most frequently asked questions about modeming and election firewall security.

1. Are Election Management Systems (EMS) connected to the internet?

No. EMS programs run on hardened computer workstations, which are not permitted to be connected to the internet. Election Reporting Manager (ERM) and Electionware, as part of the EMS, are never exposed to the internet. Only the Data Communications (SFTP) server, which sits behind the firewall in what's known as the DMZ, has any connection to the internet. Results reports and data exported from ERM/Electionware are copied to removable media when transferred outside of the secure EMS for external results reporting.

2. How does ES&S protect election management systems that receive unofficial results by modem?

ES&S uses industry best practices to protect the Data Communications server (sometimes referred to as the Results Management System, or RMS) and EMS network segments. This is done through network segmentation, stateful packet inspection, and restricting access to ports and protocols required for secure election night results transmission.

Firewalls are configured to only allow inbound connections on the DMZ network segment to traffic required for results transmission using industry-leading network security equipment. No other inbound or outbound connections are allowed based on the firewall configuration's script tested by Voting System Testing Labs (VSTLs) and certified by states. Furthermore, the firewall is configured to use a VSTL tested and State certified firewall hardware, firmware and configuration script.

On the internal network, only the EMS can initiate a data transfer connection to the Data Communications server. This is accomplished via a specific network port on a specific IP address per the certified configuration of the firewall. Per the firewall rules and certified configuration, direct connectivity from the outside (Internet) to the inside EMS network does not exist.

3. Who maintains the firewall located at a jurisdiction's election headquarters?

ES&S performs the initial firewall installation for the majority of our customers who use modem transmission to ensure the firewalls are configured to the certified configuration. Once implemented, the ongoing EMS network administrative responsibility shifts from ES&S to the jurisdiction. By secure design, no remote management access is enabled on the firewall. All management duties must be performed while physically on-site at the firewall location and locally connected to the firewall. Due to the State certified configuration, changes and updates to the firewall are prohibited outside of a state-approved Engineering Change Order (ECO) or new certified ES&S Voting System release. When changes to the firewall are approved by the State, ES&S works with jurisdictions to install the approved changes and confirm the certified functionality of the overall EMS.

4. Can a hacker break through a firewall left up and running?

Highly unlikely. One good analogy might be this: a homeowner who invests in all the latest locks and alarm systems but forgets to stop delivery of the newspaper when he's out of town. Burglars can't get into the house, but they might try because they can see a potential target. Also, remember that these are unofficial results. The physical ballots and printed results tapes are protected at all times.

5. What can jurisdictions do to further increase the security of unofficial modem transmissions?

ES&S strongly recommends that jurisdictions follow the Principle of Least Privilege and only power on and connect the firewall to external telecommunication networks when being tested or when in actual use.

6. Does ES&S have plans to make modeming of unofficial election night results even more secure?

Our most recently certified configuration for jurisdictions that wish to send unofficial results on election night incorporates Verizon (Zero Tunnel) Private Network. With Verizon Private Network, neither the firewall nor the Data Communications server in the DMZ are connected to the internet. All transmissions stay on the Verizon Private Network and never connect to the public internet. Only Verizon Private Network certified devices are used in the private network architecture. Verizon Private Networks are specifically designed for high-security applications in critical infrastructure environments. By design, public access does not exist with this architecture, resolving any concerns that your voting system is exposed to outside access. This solution has been tested by federally accredited voting system test laboratories and proven in a number of recent implementations. The Verizon Private Network is available now through Verizon. ES&S is currently working to obtain state certification approval for all of our modeming and regional reporting customers.