Frank LaRose
Ohio Secretary of State

BOOSTING ELECTION SECURITY

New Election Security Upgrades Will Make Ohio a Model for the Nation

Elections are critical infrastructure, and must be managed that way: In January of 2017, the U.S. Department of Homeland Security (DHS) designated Election Infrastructure as part of the nation's critical infrastructure. By its very nature, each and every election system is vulnerable to ever changing security environments. By implementing a cyber-defense posture that is a model for the nation, we will be in the best possible standing to deter any threats to our election system, both foreign and domestic.

The key to enhanced security is greater redundancy. A comprehensive, multi-faceted security strategy within our local boards of elections is necessary to provide the redundancy required of a strong election system infrastructure. Secretary LaRose issued a new directive for county boards of elections that serves as an aggressive execution of that approach.

Secretary LaRose's directive requires county boards of elections to implement significant security upgrades. These upgrades will be funded by the Help America Vote Act. The requirements include the following:

I. Install Albert intrusion detection devices, provided by the Ohio Secretary of State's office, for the network of each county board of elections and election system vendors that do not already utilize one. Albert devices will provide security alerts to the county boards if there is a network intrusion.

II. Conduct an assessment and annual training on cybersecurity and physical security.

III. Conduct criminal background checks of permanent board of elections employees and vendors or contractors that perform sensitive services for the board of elections.

IV. Begin utilizing the domain-based message authentication, reporting & conformance system, an email service that assists board staff with identifying whether an email is from a legitimate source and helps prevent email spoofing.

V. The Secretary of State's office will provide counties with the Security Information and Event Management (SIEM) Logging system. SIEM will serve as a figurative "Black Box" tool, similar to the device used in passenger airplanes, within the county's computer system, collecting security data from network devices, servers, domain controllers, and more. In the event of an intrusion, this will allow the BOE to know what activity was undertaken by the attacker.

VI. Require the boards to request the following services from DHS by July 19, 2019:

a. Risk and Vulnerability Assessment. This onsite assessment gathers data and "combines it with national threat and vulnerability information" to detect vulnerabilities in network security. After completing the assessment, DHS provides a final report with its findings and recommendations for improving network security controls.

b. Remote Penetration Testing. DHS provides this service remotely to identify vulnerabilities in externally accessible systems. After completing testing, DHS provides a final report with its findings and recommendations.

c. Validated Architectural Design Review. This review is designed to develop a detailed representation of the communications and relationships between devices to identify anomalous communication flows. Following the review, a participating organization will receive a report that includes discoveries and recommendations for improving organizational operations and cybersecurity.

d. Cyber Threat Hunt. DHS will perform an in-depth review on site at the board of election to determine if a network compromise has occurred.

While the demands are significant, county boards are already getting it done. Boards of Elections in Wood, Miami, and Hocking counties volunteered to serve as pilot counties for this directive several weeks ago. Their efforts have shown a keen ability to accomplish the necessary tasks and enhance their security posture as required.

OUTCOME: Security Directive 2019-08 issued by Secretary LaRose puts Ohio in a strong position to serve as *the* national leader in election security. While the demands are significant, they provide the redundancy necessary to ensure Ohio's election systems are prepared and in the best possible position for the 2020 election.