



State Representative Bernie Willis

District 74

H.B No. 472- Sponsor Testimony

Ohio House Committee on Homeland Security

1 May 2024

Chairman Ghanbari, Vice Chair Plummer, Ranking Member Thomas, and members of the House Homeland Security Committee, thank you for the opportunity to allow Representative Peterson and I to provide sponsor testimony on H.B. 472. This proposed legislation offers a comprehensive voter registration, tabulation and cybersecurity reform initiative aimed at addressing critical issues within our electoral system. Our proposal encompasses a wide range of solutions targeting various areas that currently challenge the integrity and security of voting processes.

Over the last 20 years, Ohio universally adopted electronic voting system products and services. In that timeframe, voter system technology widely expanded, and threats grew exponentially. Yet voting systems responsible for casting and tallying votes still possess many of the same security weaknesses computer scientists found in them 20 years ago, vulnerabilities that allow skilled actors to potentially alter votes without leaving any trace. If your bank was still using “voluntary” cybersecurity standards from 20 years ago, would you feel that your accounts were secure?

Consolidation of Vendors in Election Industry Heightens Vulnerability to Cyber Attack

In 2019, the Brennan Center for Justice published a report titled, “*A Framework for Election Vendor Oversight*,” citing that **80% of voting systems in use today are under the purview of three vendors**. “A successful cyberattack against any of these companies could have devastating consequences for elections in vast swaths of the country.” It takes just one software update injected with malicious code or capability developer to introduce weak software design for bad actor linked to China or Russia to compromise and exploit a system undetected.

Enhanced Voting System Cybersecurity Certification Builds Off Prior Legislation

In 2019, the Ohio House happened to also pass Senate Bill 52 unanimously (92-0), which created the Ohio Cyber Reserve, an all-volunteer, highly trained and vetted professional cyber security force under direction of the Adjutant General. At the time, our *Sec of State noted in his proponent testimony*, “By its very nature, every election system is vulnerable to the ever-changing security environment, 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 and be prepared to respond should an emergency occur.” That statement is even MORE true today as cybersecurity threats have continued to evolve.

Evolved Cyber Attacks Drive Change to Cyber Posture – Solar Winds Compromise

Until 2020, an argument could be made that if a voting system was not connected to the internet, the system remained secure from external interference. However, with the advent of the 2020 Solar Wind Attack, over 300,000 customers of IT management products and services were affected by undetected malicious software targeting customer update services and developer supply chains. The significance of the Solar Wind attack cannot be underscored for election systems which also use various IT management products and business solutions updated through automatic or remote software update services.

CISA April '24 Cyber Attack and Vendor Compromise

Just this month, the same nation-state actor assessed to have attacked Solar Winds, successfully compromised a business solutions partner for the U.S. Cybersecurity and Infrastructure Security Agency (CISA), and stole thousands of credentials and authentication certificates. Considering the current partnership between Ohio’s election officials and CISA for network monitoring security services of elections systems, how can Ohio’s constituents derive confidence or certainty that Ohio’s elections networks and services are now not under credible threat, exposed or vulnerable? The solution is to permit independent third-party security assessment reviews of voting systems to identify, report and correct vulnerabilities, not wait for a breach or compromise that may never be identified or reported.

Executive Order 14028 - Enhanced Vendor Risk Assessment Certification Criteria

Recognizing the evolving threat landscape, the White House in 2021 issued **Executive Order 14028, “improving the Nation’s Cybersecurity.”** At its core, this EO directed the development of standards, procedures and criteria for the security and integrity of software supply chain security for systems designated as “critical infrastructure.” The enhanced security criteria in this legislation is based on the intent of this order.

H.B. 472 Cybersecurity Provisions and Impact

Voting System Security Assessment Certification Standards:

H.B. 472 would establish a military-grade State-wide certification standard for all voting systems based on federal security development guidelines and National Institute of Standards Technology criteria. Ohio’s cybersecurity practices implement the most up to date enhanced risk assessment

framework in the country for voting system examination. This provides a needed update to voting system security baseline standards derived from 2005.

Independent 3rd Party Credentialed Cyber Security Review Assessments:

This provision implements enhanced voting system certification standards by employing a third-party security reviewer. By shifting technical system analysis and examination of voting systems to the Ohio Cyber Reserve, Ohio gains a credentialed reviewer and builds upon an asset put in place by the legislature to identify system security vulnerabilities and assist with critical infrastructure protection.

Voting System Procedure Opt-In:

Ohio touts itself as a “bottom-up run” election state. By placing self-determination for a majority of a county electorate to choose a voting system method, H.B. 472 clarifies ambiguity in existing law that neither requires counties adopt electronic voting system use nor restricts an alternative type of or use. In a high threat security environment of today, counties must have options and take direct action in the event an electronic voting system is withdrawn from certification or desire to activate a contingency and recovery plan should disruption to grid or polling site connectivity take place.

Voter Registration System Upgrade – Blockchain Digital Ledger

Finally, this landmark legislation introduce adoption of a blockchain digital ledger capability into the Statewide and all Counties Voter Registration Databases. Blockchain functionality records all voter record transaction history which cannot be overwritten, unlike existing databases. This upgrade assures data record integrity and practical controls to enable timely audit playback in the event of system compromise. Perhaps more importantly election administrators are alerted to alteration or evidence tampering of official voter records and can back it out to recreate the correct record. THIS is now your money is protected. Your vote deserves the same level of technology.

Closing Thoughts

2024 reflects a more precarious cyber security environment than at any other time in our nation’s history. We face an alliance of hostile nation state actors’ intent on sowing discord and distrust to our Democracy and unstable border situation. These concurrent threats prompt the need for legislation to safeguard our election system critical infrastructure through federally recommended cybersecurity measures and criteria in this bill. ***Until we adopt higher security standard certification criteria for our critical infrastructure election systems backstopped by independent credentialed cybersecurity reviews, anti-tamper evidence features in our registration databases and public disclosures of findings, the public cannot be assured of the integrity of our voting systems.***

I stand before you today as an advocate for critical reforms aimed at strengthening the integrity and efficiency of Ohio's already strong election system. The challenges facing our voter registration systems and cybersecurity standards demand immediate attention, and it is imperative that we address them with quick action.

By implementing these measures, we can significantly elevate the integrity and efficiency of our election system, fostering clearer transparency, accountability, and accuracy in our elections. As elected officials, it is incumbent upon us to enact laws that safeguard our election systems and restore a higher level of public trust in our democratic processes.

Thank you again for your attention and consideration. Let us stand united in our commitment to upholding the principles of democratic elections in our Republic and securing the future of Ohio's election system. Representative Peterson and I are happy to answer any questions that you have at this time.