NASS
National Association
of Secretaries of State

UPDATED February 27, 2020

ISSUE BRIEFING: Securing Elections Against Cyber Threats

The Issue: 40 members of NASS serve as their state's chief election official. Paramount to this role is safeguarding the integrity of the elections process. Securing elections from a range of threats and building a resilient system has long been a priority for Secretaries of State. Recent foreign efforts to interfere in US elections have led to an increased focus on election security by all levels of government, the private sector and non-profits. All 50 states consider their election infrastructure and processes to be a target for bad actors.

Due to this, states have made significant progress in implementing security controls, resiliency measures, training and other efforts to manage the risk to election systems. As US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Director Chris Krebs has said before Congress, "the 2018 midterms were the 'most secure' in modern US history." Secretaries of State recognize election security is a race without a finish line. They are operating in an evolving threat landscape and are continuously engaged in this effort.

What has been done?

Election Infrastructure Subsector Government Coordinating Council (EIS-GCC)
Election infrastructure was designated part of the nation's critical infrastructure in January 2017. Consequently, an Election Infrastructure Government Coordinating Council (EIS-GCC) was formed to facilitate coordination between federal, state and local governments. The EIS-GCC has 29 members, of which 24 are state and local election officials. Eight are representatives of NASS. Among its most important tasks, the EIS-GCC maintains protocols for threat information sharing and incident reporting related to elections. The EIS-GCC encourages adoption of the protocols across all election officials and industry providers.

Election Infrastructure Sharing and Analysis Center (EI-ISAC)
All 50 states as well as about 2500 local jurisdictions are members of the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) which is sponsored by DHS. Through the EI-ISAC, states were provided with Albert sensors to track network traffic and detect anomalies. The Albert sensor program has improved threat detection for individual election offices as well as situational awareness across the community. The EI-ISAC also facilitates information sharing, analyzes information to report trends and provides cybersecurity and incident response services.

State Efforts
Secretaries have expanded IT and cybersecurity teams within their offices. They have also established partnerships around election security with the federal government, National Guard, other state government agencies, private sector firms, universities and civic-minded non-profits.

- Collaboration with National Guard
    - More than 20 states have partnered with their National Guard on election security. Guard units have assisted with assessments and provided surge support for incident response. Other states are exploring National Guard partnerships. States have varying levels of opportunity to partner with the Guard due to differences across states in Guard capabilities and policy landscapes.

- Outreach to Local Election Officials
    - State election offices protect elections by providing support to local election offices. States have helped local offices replace and update systems, provided cyber hygiene and incident response training, implemented two-factor authentication for access to statewide voter registration databases, supported risk assessments and more. Several states have cyber navigator or cyber liaison programs through which they hire cybersecurity professionals who travel to localities to provide "boots-on-the-ground" support.

- Safeguarding Infrastructure
    - Secretaries have also focused election security efforts on hardening infrastructure. States have helped support the replacement and modernization of voting systems, voter registration systems and other IT systems to optimize security. States are also utilizing services provided by CISA including cybersecurity assessments, detection and prevention as well as implementing recommended security controls.

- Audits
    - Many states have recently implemented or expanded upon procedures that help verify the integrity of an election including technology audits, process audits and post-election tabulation audits.

Federal Funding

Federal funding appropriated by Congress, and distributed by the US Election Assistance Commission (EAC) helps states meet their unique needs to further invest in election security protections, personnel and systems.

- Federal Funding for Election Security
    - In 2018, Congress appropriated the remaining $380 million in Help America Vote Act (HAVA) funds. In 2019, Congress appropriated an additional $425 million in payments to states. Both sets of funds are being used to support and expand the state efforts discussed in the previous section.

Looking Forward

Election security is not a goal to be accomplished for one election. Rather, it requires ongoing efforts. State efforts described above will persist and expand. Securing elections requires a whole-of-society approach. All levels of government will continue to collaborate and share information with each other, election industry providers and non-profit organizations that support elections. Additionally, securing elections will require ongoing investment from all levels of government. Election officials will continue to work with policymakers to secure stable funding for election security.

Voters also play a key role in protecting our elections. Voters should be aware of efforts to undermine our democracy but should also know they can help safeguard democracy by registering to vote, voting and serving as a poll worker. A goal of our adversaries is to undermine confidence to discourage participation. The most important way to combat interference is to participate.

For additional questions on this issue, please contact NASS: (202) 624-3524 or lforson@sso.org.