Last Updated: July 21, 2017

ISSUE BRIEFING: Securing Future Elections Against Cyber Threats

What Are the Threats? Concerns have been raised about foreign attempts to compromise our nation's election systems through cyberattacks. In January 2017, the U.S. Department of Homeland Security designated state and local voting systems as ***critical infrastructure*** in order to offer a federal response to such threats. Secretaries of State are bolstering cybersecurity and resilience levels for future elections by focusing on key digital components of their state systems: voter registration databases, election management systems, election night reporting systems and electronic voting machines.

States Taking a Proactive Approach. Secretaries of State are committed to working with their federal, state and local partners on a voluntary basis, including the U.S. Election Assistance Commission (EAC) and the U.S. Department of Homeland Security, to solicit input on threats and share information on risk assessment and threat mitigation in our elections. Additional steps may be taken based upon credible or specific threats that are identified. Secretaries of State are also working in collaboration via the NASS Election Security Task Force, created for sharing resources, best practices and technical advice between states. Areas of shared state interest include:

- Establishing clear and effective structures for threat and intelligence information-sharing, victim notification processes and cyber incident response
- Identifying threat mitigation practices and state legislation/policy trends for consideration
- Conducting risk assessments and implementing continuous vulnerability assessments
- Ensuring that election offices have sufficient equipment, technical support and resources to maintain a sound security posture for their computer-based systems
- Fostering a culture of risk awareness with strong cyber hygiene practices

Areas of Shared State Interest

1) *Establishing clear and effective structures for threat and intelligence information-sharing, victim notification processes and cyber incident response, including:*

    - Obtaining federal government security clearances for Secretaries of State/Chief State Election Officials in order to access timely threat information to protect election systems.
    - Improving government processes for notifications regarding system attacks and breaches.
    - Establishing a Critical Infrastructure State Government Coordinating Council to interface with federal agencies regarding election security issues.
    - Leveraging MS-ISAC/State Fusion Centers for continuous monitoring, threat detection and incident awareness/response.
    - Developing state-specific frameworks for cyber incident response, in the event of a major attack.

2) Identifying threat mitigation practices and state policy trends for consideration, including:

- Under a risk-based model like the NIST Cybersecurity Framework, some states are trying to develop more of an enterprise mentality to improving cybersecurity coordination and response.

- Reviewing/updating policies for back-up paper ballots and equipment, paper printouts/records for polling place use, post-election audits, back-up voter lists (paper and electronic) and voter data security.

3) Conducting risk assessments and implementing continuous vulnerability assessments, including:

- Regularly monitoring election system threats and vulnerabilities to defend any related cyber networks against attacks, including phishing scams, malware, denial-of-service attacks and other common practices employed by malicious actors.
- Working with in-house IT advisors, private security partners, state CIOs/CISOs, Homeland Security Advisors, the Department of Homeland Security and others to ensure that state election systems are secured with technologies and standard operating practices that can successfully diagnose potential cyber threats, track cyberattacks, provide mitigation options and enhance the resilience of state systems.
- Documenting and reviewing all security procedures/systems, including pre- and post-election protocols and testing procedures, physical security and chain of custody policies and response to reported hardware/software issues.

4) Ensuring that election offices have sufficient equipment, technical support and resources to maintain a sound security posture for their computer-based systems, including:

- Consulting with key stakeholders (ie. Members of Congress, Governor, state legislators, state CIO/CISO) regarding current levels of investment in state and local election infrastructure. Request cybersecurity briefing from Governor/State CIO or CISO.
- Replacing aging voting equipment that is nearing end of life, no longer meets state testing and certification requirements, or will soon fail to meet such requirements due to lack of technical support/replacement parts.
- Bringing laws and policies guiding election administration into compliance with existing legal exemptions for critical infrastructure information-sharing under federal law.

5) Fostering a culture of risk awareness with strong cyber hygiene practices, including:

- Training or guidance on cyber hygiene protocols for elections officials, along with establishing clear communication protocols between state-local officials.
- Providing guidance on procedures for reporting election issues and security-related incidents (i.e. state hotlines, poll worker guidance, state task force, DHS/FBI coordination, state fusion center with law enforcement).

What Else Will Combat Foreign Threats? Keeping elections state and locally-run (decentralized), keeping voting equipment offline and leaving voting machines unnetworked, keeping voter lists clean and up-to-date and convincing more Americans to simply take part in voting and volunteering at the polls.

For additional questions on this briefing, please contact NASS: (202) 624-3525 or nass@sso.org.