NASS

National Association of Secretaries of State

UPDATED February 10, 2020

ISSUE BRIEFING: Planning for Cyber Incident Response

The Issue: Despite a state or entities' best efforts, perfect cybersecurity is impossible. Therefore, despite prevention mechanisms, cyber incidents can happen. Planning ahead for how to respond to cyber incidents can, however, limit their damage. Cyber incident response plans can be built into broader incident response and recovery plans, such as continuity of operations plans. Or, they can be separate but complementary plans. You should work with your partners (e.g. other state agencies and local election offices) to create statewide plans and/or complementary plans.

What does a Cyber Incident Response Plan entail?

Cyber incident response plans usually include the following elements:

- The definition an incident (and levels of severity, if appropriate);
- A notification schedule for whom to notify in what order (please refer to the GCC's Election Infrastructure Subsector Threat Information Sharing and Incident Reporting protocols for election-related cyber incidents);
- Assigned roles and responsibilities;
- Decision trees for how to remediate and/or who to call for help with remediation; and
- Legal implications to consider for potential incidents.

Where do we start?

Below is a list of resources that can help create an incident response plan. It is important to practice implementing your plan and revise it based on lessons learned – see the NASS issue briefing on tabletop exercises. NASS members can also contact NASS to receive examples of cyber incident response plans from other state offices.

- Election Infrastructure Sharing and Analysis Center's Cyber Incident Checklist
- National Association of State Chief Information Officer's Cyber Disruption Response Planning Guide
- National Institute of Standards and Technology's Computer Security Incident Handling Guide
- U.S. Department of Homeland Security Cybersecurity and Infrastructure Agency's Cyber Incident Detection & Response Desk Reference (Forthcoming)
- U.S. Department of Homeland Security's Best Practices for Continuity of Operations (Handling Destructive Malware)
- U.S. Department of Homeland Security's Incident Handling for Election Officials Guide
- U.S. Department of Homeland Security's National Cyber Incident Response Plan
- U.S. Election Assistance Commission's Cyber Incident Response Best Practices

What about communicating with the public?

Although different than cyber incident response plans, which focus on how to mitigate and respond to incidents, it is also essential to have a cyber incident communications plan. Cyber incident communications plans can be built into cyber incident response plans and include internal and external communications. Alternatively, organizations may have a separate plan for external communications during and after a cyber incident. If so, it should complement your cyber incident response plan. Harvard's Belfer Center provides a cyber incident response communications plan template for state and local election officials.

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