What The States Are Doing on Election Security

Amy Cohen, Executive Director

What is NASED?

- NASED is the only professional organization for state election directors
- Members are from all 50 states, DC, and the territories
Timeline of Events

- Early Summer 2016: Arizona and Illinois
- August 2016: State CIOs notified about potential issues with DSOS
- October 7, 2016: ODS and CISO person communicates
- November 8, 2016: Election Day
- January 6, 2017: Elections are declared critical infrastructure
- September 27, 2017: Initial meeting of Elections Infrastructure Sector Coordinating Council
- October 17, 2017: Initial meeting of Elections Infrastructure Sector Coordinating Council
- December 14, 2017: Initial meeting of Elections Infrastructure Sector Coordinating Council
- March 23, 2018: Consolidated Appropriations Act of 2018 signed into law

Pre-Existing Efforts

- Logic and accuracy testing of voting machines
- Voting machines are dedicated technology
- **Voting system standards**
  - Decentralization of election administration means there is no single system to take down or single location to attack
- Secure physical storage
- Canvasses, recounts, and audits...oh my!
Leveraging Federal Funds

- The remaining $380 million of Help America Vote Act funds were appropriated in March 2018
- 100% of the funds have been distributed to the states
- States have given the Election Assistance Commission narratives and a budget for spending the money
- The majority will be spent on enhancing election security at the state and local levels

EI-ISAC

- Only four of Idaho’s 44 counties are in the EI-ISAC
- ISAC participation doesn’t just benefit you – you’re helping your colleagues at the state and local level across the country
- The ISAC can assist with incident response, technical training, and provides other services
- States are working with the ISAC to install ALBERT monitors at the state and local levels
Working with the National Guard

- National Guard offers cybersecurity professionals trained by the National Guard
- States are taking advantage of the National Guard’s cybersecurity expertise in varying ways
  - Analysis
  - Running trainings
  - Conducting assessments

In-State Resources

- Departments of technology/CIOs offer many services comparable to DHS services
- Working with universities to take advantage of expertise
Working Groups and Trainings

- County and state election officials and IT staff working together to develop guidelines and best practices for their colleagues
- Restricting access to necessary systems until users have taken cybersecurity trainings
- Table Top Exercises and statewide training opportunities

Two-Factor Authentication
Phishing Exercises

Spoofing is when a bad actor impersonates a legitimate email sender.

DMARC prevents spoofing by allowing the recipient of an email to “check” with the sender’s domain to make sure the email meets certain criteria before the email is accepted, quarantining those emails that do not meet those criteria.

All federal domains must use DMARC and some states do, too.
Free Resources

- Athenian Project by Cloudflare
- Project Shield from Google
- 1Password
- EI-ISAC

Questions?

Amy Cohen | acohen@nased.org | @NASEDOrg | www.nased.org