
# Securing Our Elections: A State and National Perspective

September 6, 2018

NASCIO
Representing Chief Information Officers of the States

# Speakers

**Keith Ingram**
President Elect, NASED
and Director of Elections,
Texas

**Geoff Hale**
Director, Election Task Force,
Department of Homeland
Security (DHS)

NASCIO
Representing Chief Information Officers of the States

NASED
NATIONAL ASSOCIATION of
STATE ELECTION DIRECTORS

# What The States Are Doing on Election Security

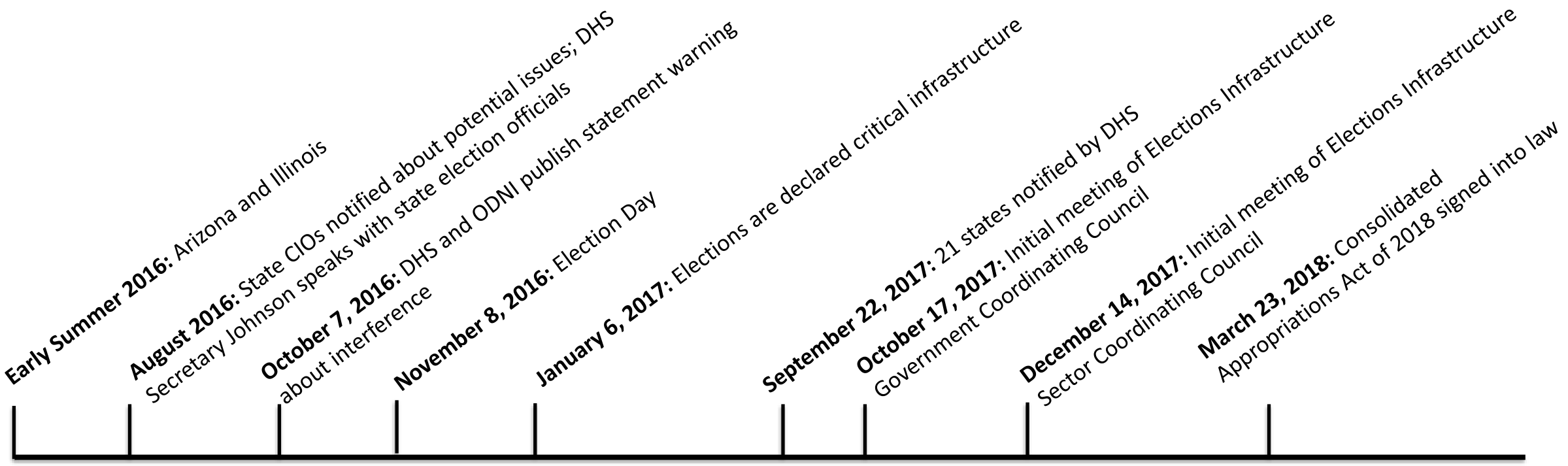
Keith Ingram, President Elect, NASED and Director of Elections, Texas

# What is NASED?

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

NASED

# Timeline of Events




NASED

# EI-ISAC

- Election offices from all 50 states, DC, Guam, and Puerto Rico participate in the EI-ISAC
- More than 1,000 local election offices - out of approximately 9,000 – are members of the EI-ISAC
- Fastest growing sector of all critical infrastructure sectors

# 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

# Pre-Existing Efforts

- Logic and accuracy testing of voting machines
- Voting machines are dedicated technology
- Voting machines themselves are not connected to the internet
- Decentralization of election administration means there is no **one** system to take down or **one** location for everything
- Secure physical storage
- Canvasses, recounts, and audits…oh my!

# Leveraging Federal Funds

- The remaining $380 million of Help America Vote Act funds were appropriated earlier this year
- 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

NASED

# 2018 Preparations in Texas

- Institution of multi-factor authentication to access the voter registration (VR) database
- Encryption of the VR data itself
- Installation of an Albert sensor on the VR database
- Working closely with DHS on cyber hygiene scans and vulnerability assessments
- Using federal money to begin assessing County election offices.
- Training materials secured and offered to the county users


# Homeland Security

Geoff Hale
Director
Election Task Force

# Election Task Force

- Our mission is to ensure that the election stakeholder community has the necessary information to adequately assess risk and to protect and detect and recover from those risks

Homeland Security

# Who are the stakeholders

- Election Officials
- Vendors
- State and local governments
- Political campaigns and candidates
- The Electorate

# What risk?

- Validity of election results
- Availability to vote
- Manipulation of voter perceptions

Homeland Security

# Elections: Critical to Democracy

"Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law."

– DHS Election Infrastructure Designation Statement, Jan. 6, 2017

## Critical infrastructure is defined as:

"Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."


Homeland Security

# Designated Critical Infrastructure

Unique designation that provides for a basis for the Department of Homeland Security and other federal agencies to:

- Recognize the importance of these systems,
- Prioritize services and support to enhancing security for such infrastructure,
- Afford the elections community an opportunity to work with each other and with the Federal Government, through government and private sector coordinating councils, and
- Communicate to the global community our intention to hold those responsible who attack these systems as violating international norms.

# DHS Services

DHS offers a broad range of services and programs to help secure election infrastructure.

Services and programs are free, and all are voluntary and provided upon request.

Contact **Cybersecurity Advisors (CSAs)** or **Protective Security Advisors (PSAs)** to identify a CSA or PSA for you, and to discuss how to select, prioritize, and sequence available services and educational programs based on specific needs.

- To contact CSAs, email: cyberadvisor@hq.dhs.gov
- To contact PSAs, email: PSCDOperations@hq.dhs.gov

Homeland Security

## Summary of DHS Services:

# Cybersecurity Assessments (Slide 1 of 2)

| Needs | DHS Services | Summary |
|---|---|---|
| Identify and Limit Vulnerabilities | Cyber Hygiene Scanning | Broadly assess Internet-accessible systems for known vulnerabilities and configuration errors on a persistent basis.<br>As potential issues are identified DHS works with impacted stakeholders to mitigate threats and risks to their systems prior to their exploitation. |
| | Risk and Vulnerability Assessment (RVA) | • Penetration testing<br>• Social engineering<br>• Wireless access discovery<br>• Database scanning<br>• Operating system scanning |
| | Phishing Campaign Assessment | • Measures susceptibility to email attack<br>• Delivers simulated phishing emails<br>• Quantifies click-rate metrics over a 10-week period |

NCCICCustomerService@HQ.dhs.gov

## Summary of DHS Services:

# Cybersecurity Assessments (Slide 2 of 2)

| Needs | DHS Services | Summary |
|---|---|---|
| Cyber Risk and IT Security Program Assessment | Cyber Resilience Review (CRR) | One-day, onsite engagement conducted on an enterprise-wide basis to give insight on areas of strength and weakness, guidance on increasing organizational cybersecurity posture, preparedness, and ongoing investment strategies. |
| | External Dependencies Management Assessment | Assesses activities and practices used by an organization to manage risk arising from external dependencies that constitute the information and communication technology service supply chain. |
| | Cyber Infrastructure Survey (CIS) | Assesses an organization's implementation and compliance with more than 80 cybersecurity controls. |

NCCICCustomerService@HQ.dhs.gov

Homeland Security

Elections Infrastructure ISAC

Provides cybersecurity support to SLTT governments.

Furthers DHS efforts to secure cyberspace by distributing early warnings of cyber threats to SLTT governments.

Shares security incident information and analysis.

Runs a 24/7 watch and warning security operations center.

Operates an election threat warning center, the Election Infrastructure-ISAC.

Funded in-part by a grant from DHS.

- For more information, see https://learn.cisecurity.org/ei-isac-registration

# What we stress for local Election Officials:

| Needs | DHS Services | Summary |
|---|---|---|
| **Identify and Limit Vulnerabilities** | **Join the EI-ISAC** | 24 x 7 x 365 network monitoring<br>Election-specific threat intelligence<br>Threat and vulnerability monitoring<br>Incident response and remediation<br>Training sessions and webinars<br>Membership in the EI-ISAC is open to all SLTT government organizations and associations supporting U.S. elections |
| **Know Your System.**<br><br>**Know Your Staff** | Cyber Hygiene Scanning* | Broadly assess Internet-accessible systems for known vulnerabilities and configuration errors on a persistent basis.<br>As potential issues are identified DHS works with impacted stakeholders to mitigate threats and risks to their systems prior to their exploitation. |
| | Phishing Campaign Assessment* | • Measures susceptibility to email attack<br>• Delivers simulated phishing emails<br>• Quantifies click-rate metrics over a 10-week period |

NCCICCustomerService@HQ.dhs.gov

Homeland Security

# What we have asked of Election officials

1. Defend
   - Ensure all aspects of voting system are air gapped
   - Update all software patches
   - Review and update system configurations & access controls
   - Manage passwords & Implement multi-factor authentication
2. Detect
   - Join EI-ISAC: https://learn.cisecurity.org/ei-isac-registration
   - Have awareness and monitoring of your systems
   - Protect and detect malware - viruses, spyware, ransomware
   - Educate employees and pollworkers
3. Recover
   - Take regular backups & test them
   - Provisional ballot/backup ballot preparation
   - Auditable ballots & conduct audits
   - Incorporate cyber incidents into your incident response plans
4. TAKE ADVANTAGE OF ALL AVAILABLE RESOURCE

Homeland Security

# Questions?

**Keith Ingram**
President Elect, NASED and Director of Elections, Texas
kingram@sos.texas.gov
@NASEDOrg | www.nased.org

**Geoff Hale**
Director, Election Task Force, Department of Homeland Security (DHS)
Geoffrey.Hale@hq.dhs.gov
https://www.dhs.gov/topic/election-security


www.NASCIO.org/CyberSeries

NASCIO
Representing Chief Information Officers of the States