DHS Election Task Force Updates

Geoff Hale,
Elections Task Force
Geoffrey.Hale@hq.dhs.gov

ETF Updates

Where we've made progress

- Services
- EI-ISAC/ National Cyber Situational Awareness Room

What we've learned

- Assessments

How this shapes our next steps

- Reaching local officials
- Exercise

DHS Cyber Services – As of 7/10/2018

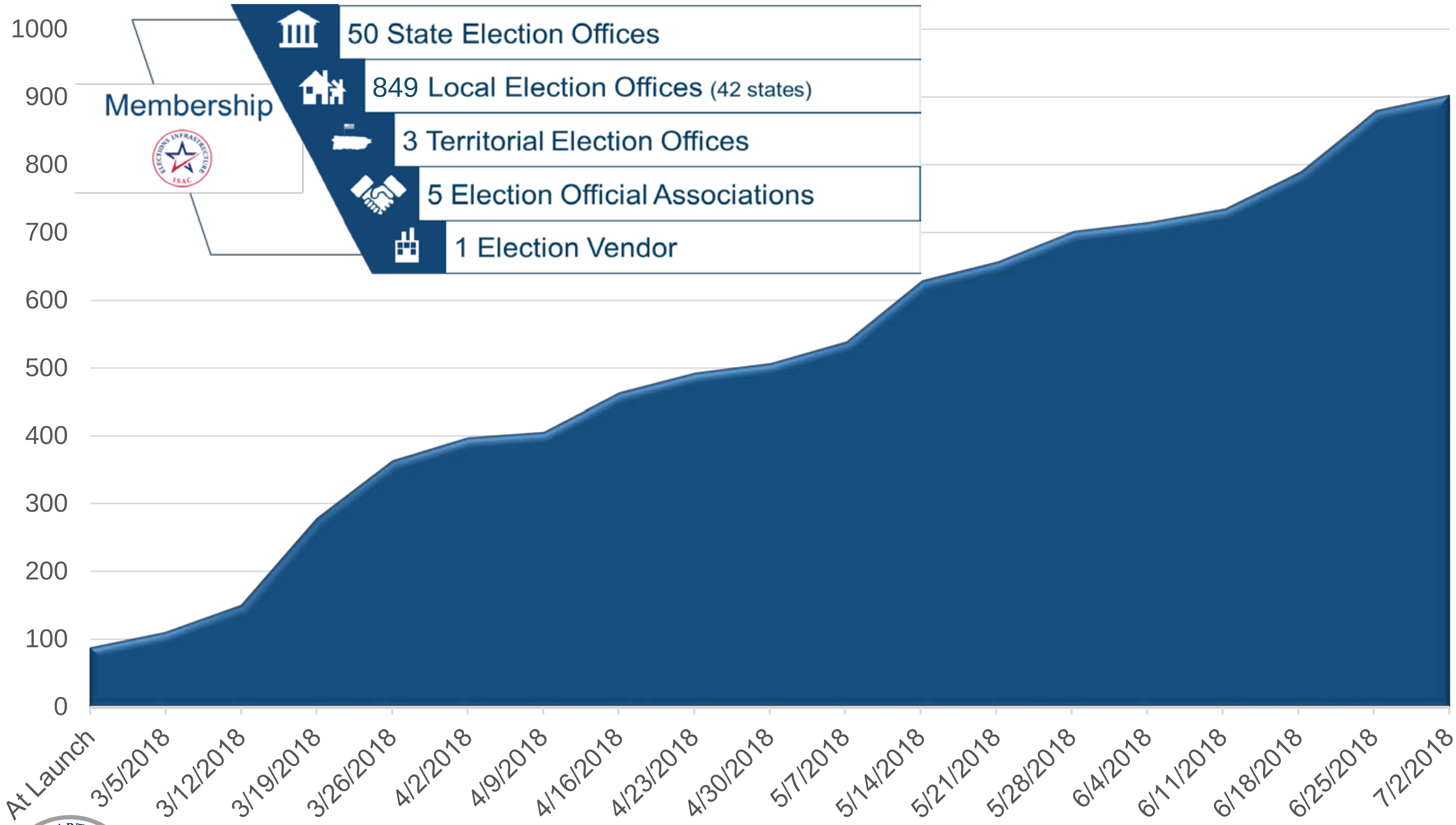
SERVICE	Total	Breakout
Cyber Resilience Review (CRR)	11	State: 8 Local: 2 Territorial: 1
External Dependencies Management Assessment (EDM)	8	State: 6 Local: 1 Territorial: 1
Cyber Infrastructure Survey (CIS)	8	State: 6 Local: 1 Territorial: 1
EI-ISAC Membership	908	State: 50 Local: 849 Territorial: 3 Association/Supporters: 6
Hunt	7	State: 5 Local: 2
Risk and Vulnerability Assessment (RVA)	35	State: 18 Local: 15 Territorial: 1 Private: 1
Phishing Campaign Assessment (PCA)	6	State: 5 Local: 1
Exercises	17	State: 17
Cyber Hygiene Scanning (CyHy)	91	State: 34 Local: 52 Private: 5

Progress of EI-ISAC

The Election Infrastructure Information Sharing and Analysis Center was adopted by GCC in February. Since that time—

- Rapid Membership Growth
- Accelerated Albert Deployment
- Availability of Supporting Membership
- Situational Awareness Room for Election Day

Membership Growth



Membership

- 50 State Election Offices
- 849 Local Election Offices (42 states)
- 3 Territorial Election Offices
- 5 Election Official Associations
- 1 Election Vendor

Homeland Security

Albert Sensor Deployment

In Progress

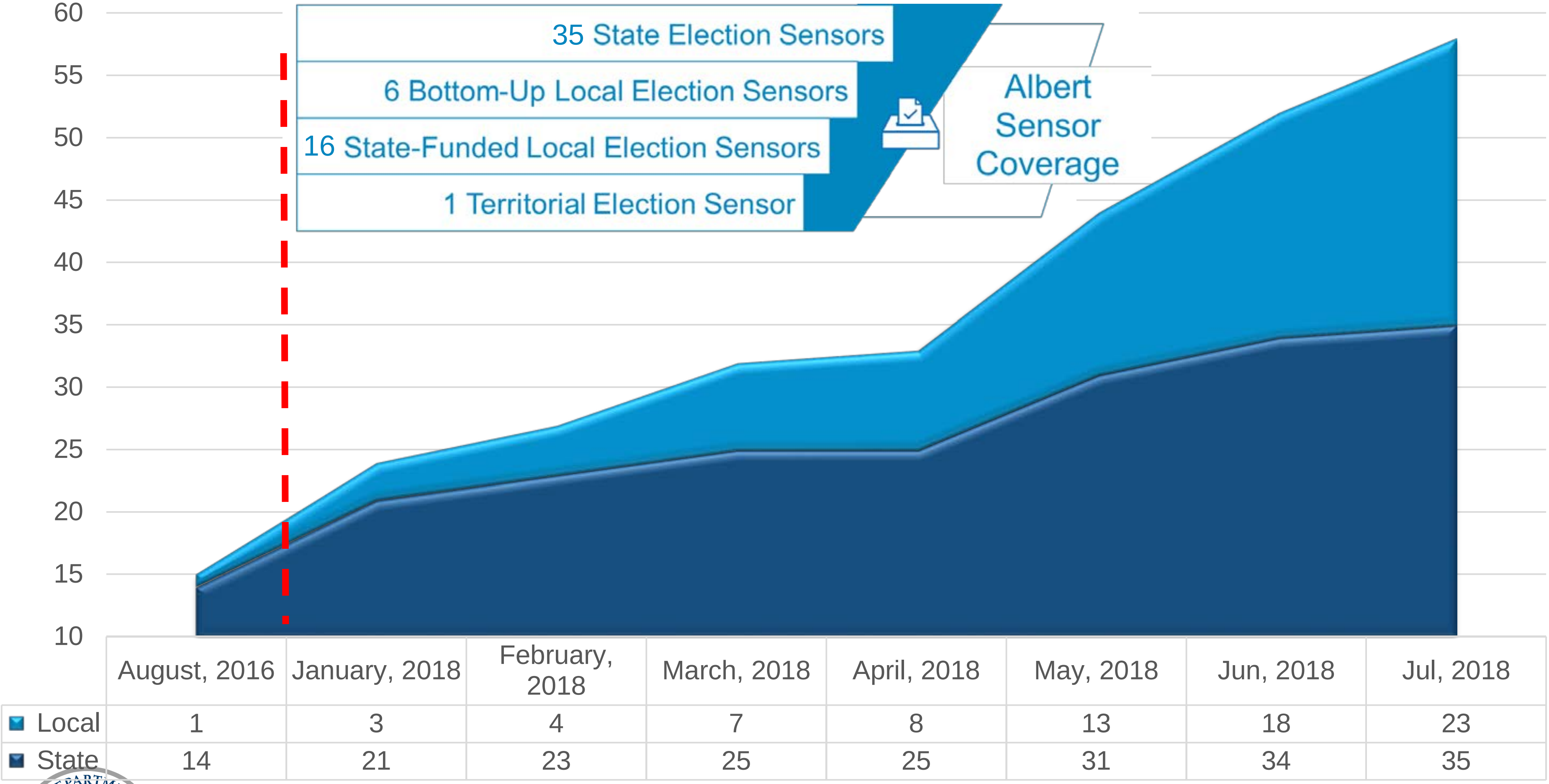
- State: 9
- Local: 9

No Information Provided:

- State: 5
- Local: 10

Sensor Declined:

- State: 2
- Local: 4



35 State Election Sensors

6 Bottom-Up Local Election Sensors

16 State-Funded Local Election Sensors

1 Territorial Election Sensor

Albert Sensor Coverage

	August, 2016	January, 2018	February, 2018	March, 2018	April, 2018	May, 2018	Jun, 2018	Jul, 2018
■ Local	1	3	4	7	8	13	18	23
■ State	14	21	23	25	25	31	34	35

Information Sharing and Engagement

Incident Notifications

Q1	Q2
13 Albert Notifications	146 Albert Notifications
4 Open Source Notifications	1 Open Source Notification
72 VMP Notifications	55 VMP Notifications
8 Reported Incidents	9 Reported Incidents
1 Incident Response	1 Incident Response

Engage Election Stakeholders

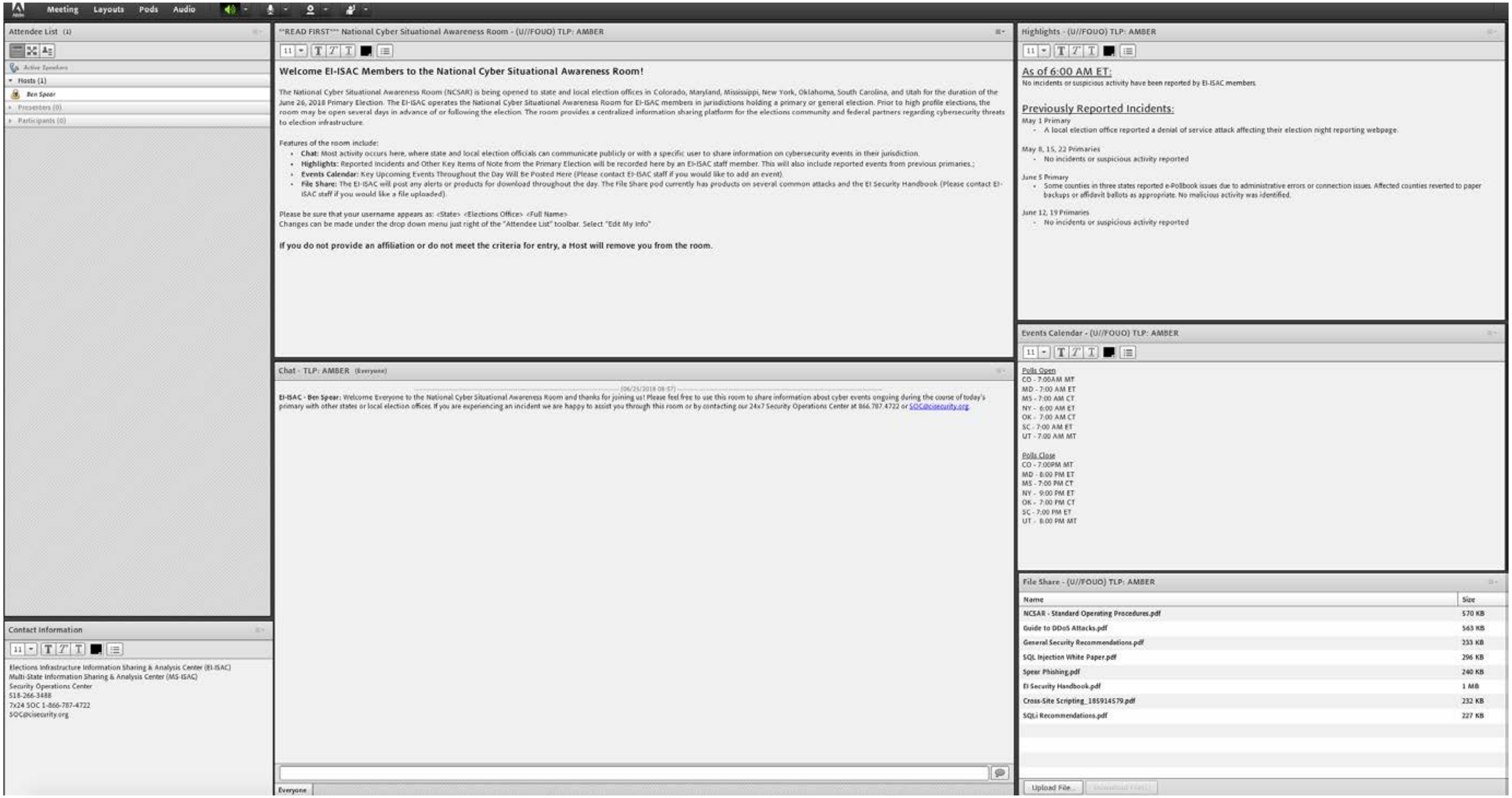
Webinars	7
Conference Briefings and TTX	26
Situational Awareness Rooms	6

Election Information Sharing Products

ELECTION PRODUCTS

Cyber Alerts	0
Weekly News Alerts	27
Cybersecurity Spotlight	11
Total Election Products Disseminated	38

Election Day Situational Awareness Room



Attendee List (1)

Active Speakers
Hosts (1)
Ben Spear
Presenters (0)
Participants (0)

READ FIRST* National Cyber Situational Awareness Room - (U//FOUO) TLP: AMBER

Welcome EI-ISAC Members to the National Cyber Situational Awareness Room!

The National Cyber Situational Awareness Room (NCSAR) is being opened to state and local election offices in Colorado, Maryland, Mississippi, New York, Oklahoma, South Carolina, and Utah for the duration of the June 26, 2018 Primary Election. The EI-ISAC operates the National Cyber Situational Awareness Room for EI-ISAC members in jurisdictions holding a primary or general election. Prior to high profile elections, the room may be open several days in advance of or following the election. The room provides a centralized information sharing platform for the elections community and federal partners regarding cybersecurity threats to election infrastructure.

Features of the room include:

- **Chat**: Most activity occurs here, where state and local election officials can communicate publicly or with a specific user to share information on cybersecurity events in their jurisdiction.
- **Highlights**: Reported Incidents and Other Key Items of Note from the Primary Election will be recorded here by an EI-ISAC staff member. This will also include reported events from previous primaries.;
- **Events Calendar**: Key Upcoming Events Throughout the Day Will Be Posted Here (Please contact EI-ISAC staff if you would like to add an event).
- **File Share**: The EI-ISAC will post any alerts or products for download throughout the day. The File Share pod currently has products on several common attacks and the EI Security Handbook (Please contact EI-ISAC staff if you would like a file uploaded).

Please be sure that your username appears as: <State> <Elections Office> <Full Name>
Changes can be made under the drop down menu just right of the "Attendee List" toolbar. Select "Edit My Info"

If you do not provide an affiliation or do not meet the criteria for entry, a Host will remove you from the room.

Chat - TLP: AMBER (Everyone)

[06/25/2018 08:57]

EI-ISAC - Ben Spear: Welcome Everyone to the National Cyber Situational Awareness Room and thanks for joining us! Please feel free to use this room to share information about cyber events ongoing during the course of today's primary with other states or local election offices. If you are experiencing an incident we are happy to assist you through this room or by contacting our 24x7 Security Operations Center at 866.787.4722 or SOC@cisecurity.org

Contact Information

Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC)
Multi-State Information Sharing & Analysis Center (MS-ISAC)
Security Operations Center
518-266-3488
7x24 SOC 1-866-787-4722
SOC@cisecurity.org

Highlights - (U//FOUO) TLP: AMBER

As of 6:00 AM ET:
No incidents or suspicious activity have been reported by EI-ISAC members.

Previously Reported Incidents:

May 1 Primary
- A local election office reported a denial of service attack affecting their election night reporting webpage.

May 8, 15, 22 Primaries
- No incidents or suspicious activity reported

June 5 Primary
- Some counties in three states reported e-Pollbook issues due to administrative errors or connection issues. Affected counties reverted to paper backups or affidavit ballots as appropriate. No malicious activity was identified.

June 12, 19 Primaries
- No incidents or suspicious activity reported

Events Calendar - (U//FOUO) TLP: AMBER

Polls Open
CO - 7:00AM MT
MD - 7:00 AM ET
MS - 7:00 AM CT
NY - 6:00 AM ET
OK - 7:00 AM CT
SC - 7:00 AM ET
UT - 7:00 AM MT

Polls Close
CO - 7:00PM MT
MD - 8:00 PM ET
MS - 7:00 PM CT
NY - 9:00 PM ET
OK - 7:00 PM CT
SC - 7:00 PM ET
UT - 8:00 PM MT

File Share - (U//FOUO) TLP: AMBER

Name	Size
NCSAR - Standard Operating Procedures.pdf	570 KB
Guide to DDoS Attacks.pdf	563 KB
General Security Recommendations.pdf	233 KB
SQL Injection White Paper.pdf	296 KB
Spear Phishing.pdf	240 KB
EI Security Handbook.pdf	1 MB
Cross-Site Scripting_185914579.pdf	232 KB
SQLi Recommendations.pdf	227 KB

What We’ve Learned from Assessments

Penetration Testing Findings (from RVAs)
Election Infrastructure Risks
Spear Phishing Weaknesses
Admin Password Reuse
Patch Management
Unsupported OS or Application
Cleartext Password Disclosure

What does it mean?

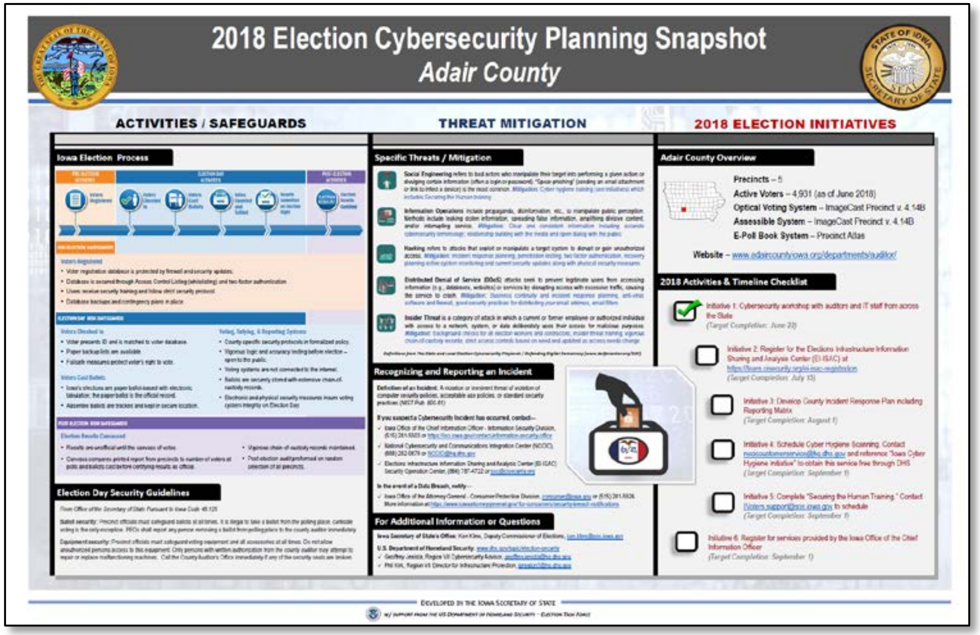
Identifying and addressing needs:

- Growing a robust dataset amplifies our understanding of risk across the sector
  - **Objective:** Expand reach
- Risks and vulnerabilities identified can be mitigated through foundational information security practices
  - **Objective:** Educate and promote basic information security practices across sector
- Information risk management & planning practices are not standard across the sector
  - **Objective:** Support education and planning efforts according to NIST Cybersecurity Framework

2018 Election Cybersecurity Snapshots

- With a goal of expanding reach to local election jurisdictions and promoting foundational security practices, DHS piloted with Iowa Office of the Secretary of State (SOS), Election Cybersecurity Posters

- Provides each county in Iowa with—
  - An illustrative document to share with leadership, regulators, and constituents describing the county's election cybersecurity activities and action plan
  - Accessible reference for cybersecurity points of contact
  - Checklist of high-impact initiatives recommended by the Iowa SOS and U.S. DHS



2018 Election Cybersecurity Planning Snapshot

Adair County

ACTIVITIES / SAFEGUARDS

THREAT MITIGATION

2018 ELECTION INITIATIVES

Iowa Election Process

Pre-Election Activities
Election Day Activities
Post-Election Activities
Voters Registered
Voters Checked In
Voters Cast Ballots
Votes Counted and Tallied
Results Submitted on Election Night
Election Results Canvassed

Pre-Election Risk Safeguards

Voters Registered

- Voter registration database is protected by firewall and security updates.
- Database is secured through Access Control Listing (whitelisting) and two-factor authentication.
- Users receive security training and follow strict security protocol.
- Database backups and contingency plans in place.

Election Day Risk Safeguards

Voters Checked In

- Voter presents ID and is matched to voter database.
- Paper backup lists are available.
- Failsafe measures protect voter's right to vote.

Voters Cast Ballots

- Iowa's elections are paper ballot-based with electronic tabulation; the paper ballot is the official record.
- Absentee ballots are tracked and kept in secure location.

Voting, Tallying, & Reporting Systems

- County specific security protocols in formalized policy.
- Vigorous logic and accuracy testing before election – open to the public.
- Voting systems are not connected to the internet.
- Ballots are securely stored with extensive chain of custody records.
- Electronic and physical security measures insure voting system integrity on Election Day.

Post-Election Risk Safeguards

Election Results Canvassed

- Results are unofficial until the canvass of votes.
- Canvass compares printed report from precincts to number of voters at polls and ballots cast before certifying results as official.
- Vigorous chain of custody records maintained.
- Post-election audit performed on random selection of all precincts.

Election Day Security Guidelines

From Office of the Secretary of State Pursuant to Iowa Code 49.125

Ballot security: Precinct officials must safeguard ballots at all times. It is illegal to take a ballot from the polling place; curbside voting is the only exception. PEOs shall report any person removing a ballot from polling place to the county auditor immediately.

Equipment security: Precinct officials must safeguard voting equipment and all accessories at all times. Do not allow unauthorized persons access to this equipment. Only persons with written authorization from the county auditor may attempt to repair or replace malfunctioning machines. Call the County Auditor's Office immediately if any of the security seals are broken.

Specific Threats / Mitigation

Social Engineering refers to bad actors who manipulate their target into performing a given action or divulging certain information (often a login or password). "Spear-phishing" (sending an email attachment or link to infect a device) is the most common. *Mitigation:* Cyber hygiene training (see initiatives) which includes Securing the Human training.

Information Operations include propaganda, disinformation, etc., to manipulate public perception. Methods include leaking stolen information, spreading false information, amplifying divisive content, and/or interrupting service. *Mitigation:* Clear and consistent information including accurate cybersecurity terminology; relationship building with the media and open dialog with the public.

Hacking refers to attacks that exploit or manipulate a target system to disrupt or gain unauthorized access. *Mitigation:* incident response planning, penetration testing, two factor authentication, recovery planning, active system monitoring and current security updates along with physical security measures.

Distributed Denial of Service (DDoS) attacks seek to prevent legitimate users from accessing information (e.g., databases, websites) or services by disrupting access with excessive traffic, causing the service to crash. *Mitigation:* Business continuity and incident response planning, anti-virus software and firewall, good security practices for distributing your email address, email filters.

Insider Threat is a category of attack in which a current or former employee or authorized individual with access to a network, system, or data deliberately uses their access for malicious purposes. *Mitigation:* background checks for all election workers and contractors, insider threat training, vigorous chain-of-custody records, strict access controls based on need and updated as access needs change.

Definitions from The State and Local Election Cybersecurity Playbook / Defending Digital Democracy ([illegible])

Recognizing and Reporting an Incident

Definition of an Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices (NIST Pub. 800-61)

If you suspect a Cybersecurity Incident has occurred, contact—

- ✓ Iowa Office of the Chief Information Officer - Information Security Division, (515) 281-5503 or https://ocio.iowa.gov/contact-information-security-office
- ✓ National Cybersecurity and Communications Integration Center (NCCIC), (888) 282-0870 or NCCIC@hq.dhs.gov
- ✓ Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) Security Operation Center, (866) 787-4722 or soc@cisecurity.org

In the event of a Data Breach, notify—

- ✓ Iowa Office of the Attorney General - Consumer Protection Division, consumer@iowa.gov or (515) 281-5926. More information at https://www.iowaattorneygeneral.gov/for-consumers/security-breach-notifications

For Additional Information or Questions

Iowa Secretary of State's Office: Ken Kline, Deputy Commissioner of Elections, ken.kline@sos.iowa.gov

U.S. Department of Homeland Security: www.dhs.gov/topic/election-security

- ✓ Geoffrey Jenista, Region VII Cybersecurity Advisor, geoffrey.jenista@hq.dhs.gov
- ✓ Phil Kirk, Region VII Director for Infrastructure Protection, [illegible]@hq.dhs.gov

Adair County Overview

Precincts – 5
Active Voters – 4,931 (as of June 2018)
Optical Voting System – ImageCast Precinct v. 4.14B
Assessible System – ImageCast Precinct v. 4.14B
E-Poll Book System – Precinct Atlas

Website – www.adaircountyiowa.org/departments/auditor/

2018 Activities & Timeline Checklist

☑ Initiative 1: Cybersecurity workshop with auditors and IT staff from across the State
(Target Completion: June 22)

☐ Initiative 2: Register for the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) at https://learn.cisecurity.org/ei-isac-registration
(Target Completion: July 15)

☐ Initiative 3: Develop County Incident Response Plan including Reporting Matrix
(Target Completion: August 1)

☐ Initiative 4: Schedule Cyber Hygiene Scanning. Contact ncciccustomerservice@hq.dhs.gov and reference "Iowa Cyber Hygiene Initiative" to obtain this service free through DHS
(Target Completion: September 1)

☐ Initiative 5: Complete "Securing the Human Training." Contact [illegible]support@sos.iowa.gov to schedule
(Target Completion: September 1)

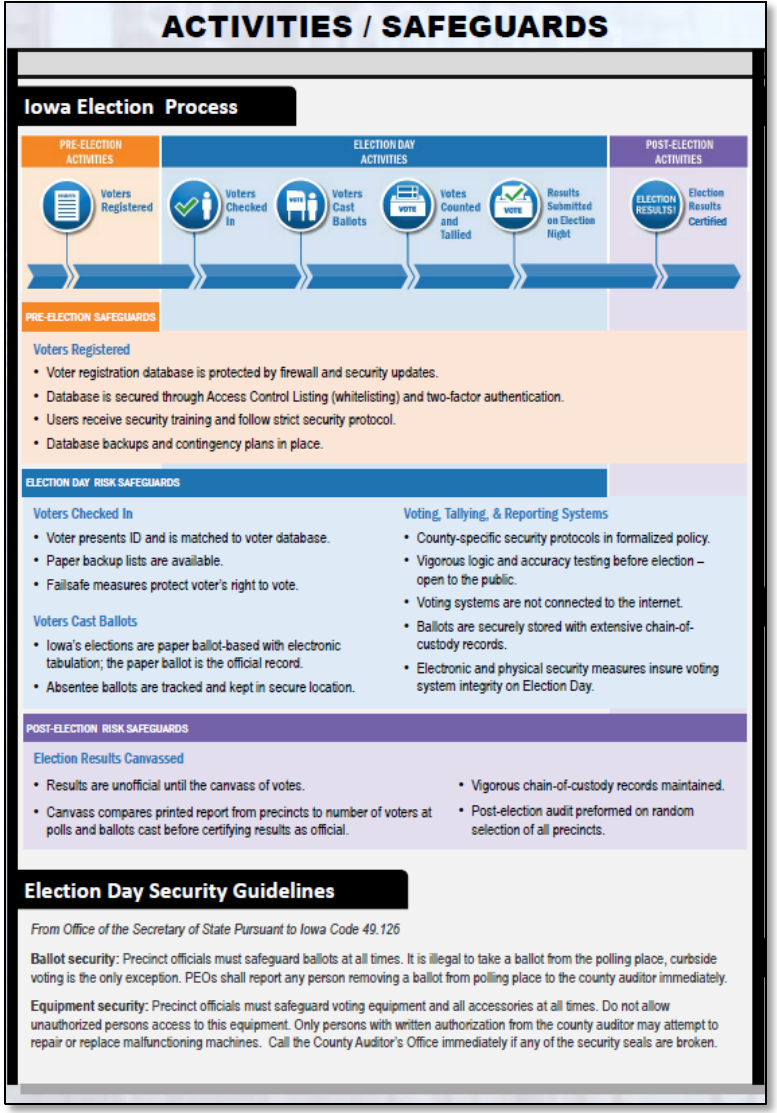
☐ Initiative 6: Register for services provided by the Iowa Office of the Chief Information Officer
(Target Completion: September 1)

DEVELOPED BY THE IOWA SECRETARY OF STATE
W/ SUPPORT FROM THE US DEPARTMENT OF HOMELAND SECURITY – ELECTION TASK FORCE

Snapshot – Activities/ Safeguards

Iowa Election Process— Lists controls and other cybersecurity safeguards in place for each phase of the election process

Election Day Security Guidelines—Reference to key Iowa policies relating to election cybersecurity



ACTIVITIES / SAFEGUARDS

Iowa Election Process

PRE-ELECTION ACTIVITIES

- Voters Registered

ELECTION DAY ACTIVITIES

- Voters Checked In
- Voters Cast Ballots
- Votes Counted and Tallied
- Results Submitted on Election Night

POST-ELECTION ACTIVITIES

- Election Results Certified

ELECTION RESULTS!
VOTE
VOTE
VOTE

PRE-ELECTION SAFEGUARDS

Voters Registered

- Voter registration database is protected by firewall and security updates.
- Database is secured through Access Control Listing (whitelisting) and two-factor authentication.
- Users receive security training and follow strict security protocol.
- Database backups and contingency plans in place.

ELECTION DAY RISK SAFEGUARDS

Voters Checked In

- Voter presents ID and is matched to voter database.
- Paper backup lists are available.
- Failsafe measures protect voter's right to vote.

Voters Cast Ballots

- Iowa's elections are paper ballot-based with electronic tabulation; the paper ballot is the official record.
- Absentee ballots are tracked and kept in secure location.

Voting, Tallying, & Reporting Systems

- County-specific security protocols in formalized policy.
- Vigorous logic and accuracy testing before election – open to the public.
- Voting systems are not connected to the internet.
- Ballots are securely stored with extensive chain-of-custody records.
- Electronic and physical security measures insure voting system integrity on Election Day.

POST-ELECTION RISK SAFEGUARDS

Election Results Canvassed

- Results are unofficial until the canvass of votes.
- Canvass compares printed report from precincts to number of voters at polls and ballots cast before certifying results as official.
- Vigorous chain-of-custody records maintained.
- Post-election audit preformed on random selection of all precincts.

Election Day Security Guidelines

From Office of the Secretary of State Pursuant to Iowa Code 49.126

Ballot security: Precinct officials must safeguard ballots at all times. It is illegal to take a ballot from the polling place, curbside voting is the only exception. PEOs shall report any person removing a ballot from polling place to the county auditor immediately.

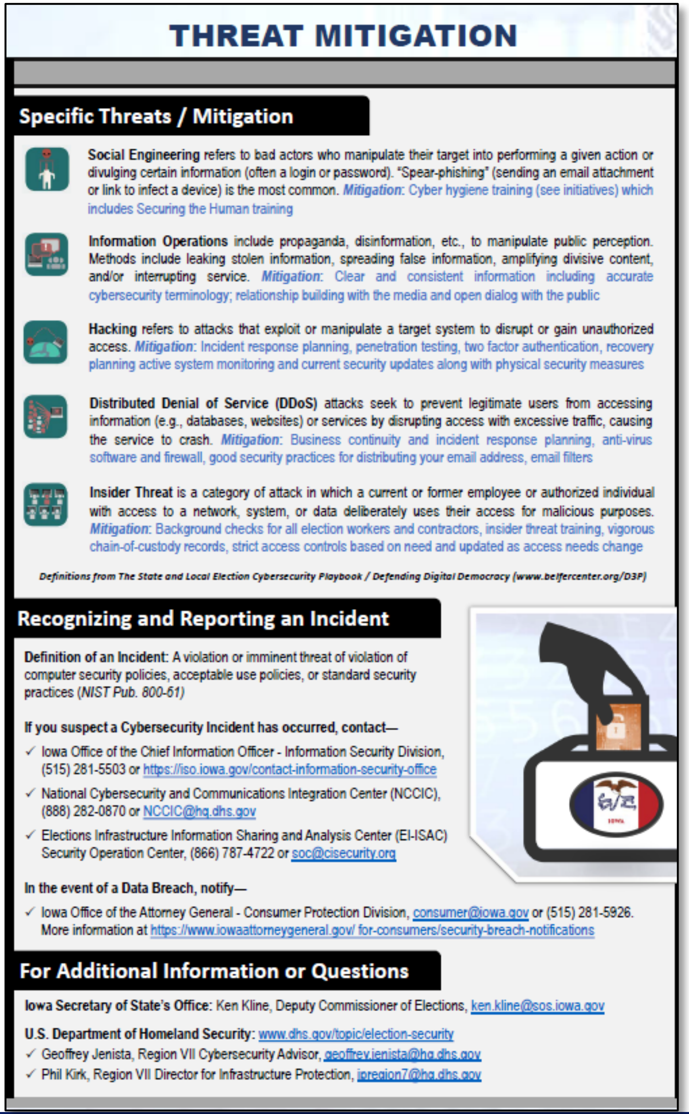
Equipment security: Precinct officials must safeguard voting equipment and all accessories at all times. Do not allow unauthorized persons access to this equipment. Only persons with written authorization from the county auditor may attempt to repair or replace malfunctioning machines. Call the County Auditor's Office immediately if any of the security seals are broken.

Snapshot – Threat Mitigation

Specific Threats/Mitigation—Description of various cyber threats to the election process along with current and planned mitigation actions

Recognizing and Reporting an Incident— Defines "cyber incident" and provides key POCs at the state and national level for incident reporting and/or assistance

For Additional Information/ Questions— POCs for obtaining additional information on state and national cybersecurity resources and initiatives



THREAT MITIGATION

Specific Threats / Mitigation

Social Engineering refers to bad actors who manipulate their target into performing a given action or divulging certain information (often a login or password). "Spear-phishing" (sending an email attachment or link to infect a device) is the most common. ***Mitigation***: Cyber hygiene training (see initiatives) which includes Securing the Human training

Information Operations include propaganda, disinformation, etc., to manipulate public perception. Methods include leaking stolen information, spreading false information, amplifying divisive content, and/or interrupting service. ***Mitigation***: Clear and consistent information including accurate cybersecurity terminology; relationship building with the media and open dialog with the public

Hacking refers to attacks that exploit or manipulate a target system to disrupt or gain unauthorized access. ***Mitigation***: Incident response planning, penetration testing, two factor authentication, recovery planning active system monitoring and current security updates along with physical security measures

Distributed Denial of Service (DDoS) attacks seek to prevent legitimate users from accessing information (e.g., databases, websites) or services by disrupting access with excessive traffic, causing the service to crash. ***Mitigation***: Business continuity and incident response planning, anti-virus software and firewall, good security practices for distributing your email address, email filters

Insider Threat is a category of attack in which a current or former employee or authorized individual with access to a network, system, or data deliberately uses their access for malicious purposes. ***Mitigation***: Background checks for all election workers and contractors, insider threat training, vigorous chain-of-custody records, strict access controls based on need and updated as access needs change

Definitions from The State and Local Election Cybersecurity Playbook / Defending Digital Democracy (www.belfercenter.org/D3P)

Recognizing and Reporting an Incident

Definition of an Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices (*NIST Pub. 800-61)*

If you suspect a Cybersecurity Incident has occurred, contact—

- ✓ Iowa Office of the Chief Information Officer - Information Security Division, (515) 281-5503 or https://iso.iowa.gov/contact-information-security-office
- ✓ National Cybersecurity and Communications Integration Center (NCCIC), (888) 282-0870 or NCCIC@hq.dhs.gov
- ✓ Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) Security Operation Center, (866) 787-4722 or soc@cisecurity.org

In the event of a Data Breach, notify—

- ✓ Iowa Office of the Attorney General - Consumer Protection Division, consumer@iowa.gov or (515) 281-5926. More information at https://www.iowaattorneygeneral.gov/ for-consumers/security-breach-notifications

For Additional Information or Questions

Iowa Secretary of State's Office: Ken Kline, Deputy Commissioner of Elections, ken.kline@sos.iowa.gov

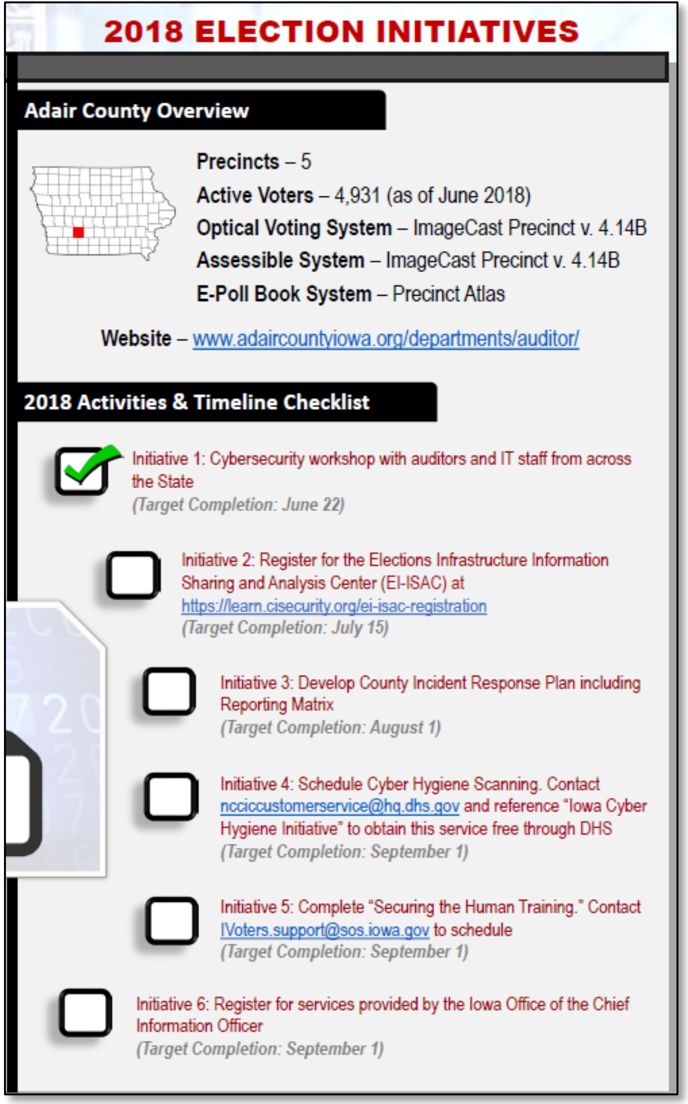
U.S. Department of Homeland Security: www.dhs.gov/topic/election-security

- ✓ Geoffrey Jenista, Region VII Cybersecurity Advisor, geoffrey.jenista@hq.dhs.gov
- ✓ Phil Kirk, Region VII Director for Infrastructure Protection, ipregion7@hq.dhs.gov

Snapshot – 2018 Initiatives

County Overview— County-specific data including number of precincts and voters, types of voting equipment, and website for election information.

2018 Activities & Timeline— Checklist of high-impact cybersecurity initiatives recommended by Iowa SOS and U.S. DHS for completion prior to the November 2018 election. Several initiatives take advantage of free services offered by the State of Iowa or U.S. DHS.



2018 ELECTION INITIATIVES

Adair County Overview

Precincts – 5
Active Voters – 4,931 (as of June 2018)
Optical Voting System – ImageCast Precinct v. 4.14B
Assessible System – ImageCast Precinct v. 4.14B
E-Poll Book System – Precinct Atlas

Website – www.adaircountyiowa.org/departments/auditor/

2018 Activities & Timeline Checklist

☑ Initiative 1: Cybersecurity workshop with auditors and IT staff from across the State
(Target Completion: June 22)

☐ Initiative 2: Register for the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) at https://learn.cisecurity.org/ei-isac-registration
(Target Completion: July 15)

☐ Initiative 3: Develop County Incident Response Plan including Reporting Matrix
(Target Completion: August 1)

☐ Initiative 4: Schedule Cyber Hygiene Scanning. Contact ncciccustomerservice@hq.dhs.gov and reference "Iowa Cyber Hygiene Initiative" to obtain this service free through DHS
(Target Completion: September 1)

☐ Initiative 5: Complete "Securing the Human Training." Contact IVoters.support@sos.iowa.gov to schedule
(Target Completion: September 1)

☐ Initiative 6: Register for services provided by the Iowa Office of the Chief Information Officer
(Target Completion: September 1)

2018 Election Cybersecurity Initiatives

☑ **Initiative 1: Cybersecurity workshop with auditors and IT staff from across the State**
(Target Completion: June 22)

☐ **Initiative 2: Register for the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) at https://learn.cisecurity.org/ei-isac-registration**
(Target Completion: July 15)

☐ **Initiative 3: Develop County Incident Response Plan including Reporting Matrix**
(Target Completion: August 1)

☐ **Initiative 4: Schedule Cyber Hygiene Scanning. Contact ncciccustomerservice@hq.dhs.gov and reference "Iowa Cyber Hygiene Initiative" to obtain this service free through DHS**
(Target Completion: September 1)

☐ **Initiative 5: Complete "Securing the Human Training." Contact IVoters.support@sos.iowa.gov to schedule**
(Target Completion: September 1)

☐ **Initiative 6: Register for services provided by the Iowa Office of the Chief Information Officer**
(Target Completion: September 1)

Tabletop The Vote 2018

Format: Open forum facilitated discussions conducted via VTC (or audio bridge)

Date: Exercise will be repeated on three consecutive days:

- 13 August: (Monday) 12:00 pm to 4:00 pm
- 14 August (Tuesday) 12:00 pm to 4:00 pm
- 15 August (Wednesday) 12:00 pm to 4:00 pm

Venues:

- FEMA Emergency Management Institute (Facilitation)
- DHS 1110 N. Glebe Road - Room 1128 (Federal Interagency Participation)
- State EOC or similar (State/County Player Locations)

Parameters:

- Focus on cyber impacts to voter confidence and integrity of elections
- Discussion will be non-technical

Tabletop The Vote 2018

- The purpose of this exercise is to assist DHS and elections stakeholders in identifying best practices and areas for improvement in cyber incident planning, preparedness, identification and response through simulation of a realistic scenario exploring impacts to voter confidence, voting operations, and the integrity of elections.

- The exercise will provide unparalleled networking opportunities for the development of information sharing relationships amongst election community stakeholders and the federal government.

- The exercise will also provide the opportunity for DHS and Federal interagency partners to exercise collaboration and information sharing practices both in steady state and in response to a cyber incident.

Tabletop The Vote 2018

Exercise Objectives

1. Discuss the preparedness of the state and county boards of election to respond to and manage cybersecurity incidents.

2. Discuss processes for identifying potential cybersecurity incidents or issues.

3. Examine information sharing processes among the state and county boards of election and with state and federal partners.

4. Explore processes for requesting state/federal incident response resources once county/state resources are exhausted.

5. Increase understanding of federal cyber risk management resources and incident response roles, responsibilities, and coordination processes.

6. Explore processes for addressing news and social media manipulation related to the conduct of elections.

7. Inform the development of state and county-level processes and plans to address elections-related cyber incidents.

EISSA@hq.dhs.gov

ElectionTaskForce@hq.dhs.gov

Geoffrey.Hale@hq.dhs.gov

FOR MORE INFORMATION