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

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

## Incident Notifications

<table>
<thead>
<tr>
<th></th>
<th>Q1</th>
<th>Q2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Albert Notifications</td>
<td>13</td>
<td>146</td>
</tr>
<tr>
<td>Open Source Notifications</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>VMP Notifications</td>
<td>72</td>
<td>55</td>
</tr>
<tr>
<td>Reported Incidents</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>Incident Response</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

## 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
## What We’ve Learned from Assessments

### Penetration Testing Findings (from RVAs)

<table>
<thead>
<tr>
<th>Election Infrastructure Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spear Phishing Weaknesses</td>
</tr>
<tr>
<td>Admin Password Reuse</td>
</tr>
<tr>
<td>Patch Management</td>
</tr>
<tr>
<td>Unsupported OS or Application</td>
</tr>
<tr>
<td>Cleartext Password Disclosure</td>
</tr>
</tbody>
</table>
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.
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.
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
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 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