Managing IT & Election Systems
Election Administrators are IT Managers

• Election Officials and their constituencies must understand that they are complex IT system managers
  ▪ Most election officials and constituencies don’t realize they manage more IT assets than any other department in the jurisdiction.
  ▪ All election officials are reliant upon vendors, contractors, or consultants and must manage those relationships.
  ▪ Voting systems are aging.

• Governance is the first step to IT Management
  ▪ Make sure the relationship between the IT and Organizational strategic goals align

• Election Officials take a risk-based approach and build resiliency in the process
The typical county election official is managing more technology than any other county department:

<table>
<thead>
<tr>
<th>Election Systems</th>
<th>Office IT</th>
<th>Software/Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Election Management Systems</td>
<td>Servers/Workstations</td>
<td>VoIP</td>
</tr>
<tr>
<td>Voter Registration Systems</td>
<td>Tablets</td>
<td>GIS</td>
</tr>
<tr>
<td>Electronic Pollbooks</td>
<td>Smartphones</td>
<td>Cloud services</td>
</tr>
<tr>
<td>Voting Devices</td>
<td>Printers/Copiers</td>
<td>Websites</td>
</tr>
<tr>
<td>Scanners</td>
<td>Fax machines</td>
<td>Social Media</td>
</tr>
</tbody>
</table>
IT Governance

• Must take a top-down approach beginning with Senior Leadership
• Create a proactive security culture
• Distribute guidance on security best practices
• Conduct training and exercises
• Review policies and procedures
• Provide authority and support to implementers
Election System Resilience

- **Elections are a system of systems, so treat them as an interconnected system**
  - Recognize that ALL systems are connected, directly or indirectly, with another system.

- **Implement Security Controls across all systems**
  - Prevention
  - Detection
  - Corrective

- **Defense in Depth**
Defense in Depth
I-TEAM

How the Russians penetrated Illinois election computers

SQL, an acronym for Structured Query Language, is a database programming language. An "SQL injection" is a common piece of cyber-trickery used to illegally gain access to government, financial, business and private computers. Experts estimate that 8 of every 10 data breaches occur as a result of SQL injection.

The favored tactic of hackers usually begins with certain commands typed on a public web form and ends with broad access to the site's server. In the case of Illinois, after hackers typed a specially-crafted code into the election database search box, records were stolen and the board had to shut down registration for ten days.

"Processor usage had spiked to 100% with no explanation," state investigators determined. "Analysis of server logs revealed that the heavy load was a result of rapidly repeated database queries on the application status page of the Paperless Online Voter Application (POVA) website" they said.
Website of State Board of Elections and Ethics Hacked by ISIS

North Carolina’s elections board provided this image to state lawmakers in a December 2017 presentation. - State Board of Elections and Ethics Enforcement
DDoS Attack Hits Knox County, TN Results Reporting Site On Election Night

By Doug Chapin  May 7, 2018
Six days after a ransomware cyberattack, Atlanta officials are filling out forms by hand

By Kimberly Hutcherson, CNN

Updated 3:00 PM ET, Wed March 28, 2018

Atlanta mayor: Ransomware an attack on us all

SOURCE: WSB

By NICOLE PERLROTH  JULY 6, 2017

The Wolf Creek Nuclear power plant in Kansas in 2000. The corporation that runs the plant was targeted by hackers. David Eulitt/Capital Journal, via Associated Press
Things that matter

Things you can control

What you should focus on
RESOURCES

DHS Cyber Security Offerings
## Summary of DHS Services: Cybersecurity Assessments

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

<table>
<thead>
<tr>
<th>Needs</th>
<th>DHS Services</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY</td>
<td>Cyber Resiliency Review</td>
<td>The Cyber Resilience Review (CRR) is a no-cost, voluntary, interview-based assessment to evaluate an organization’s operational resilience and cybersecurity practices.</td>
</tr>
<tr>
<td>PROTECT</td>
<td>External Dependencies Management Assessment</td>
<td>The External Dependencies Management (EDM) assessment is a no-cost, voluntary, interview-based assessment to evaluate an organization’s management of their dependencies.</td>
</tr>
<tr>
<td>DETECT</td>
<td>Cyber Infrastructure Survey</td>
<td>The Cyber Infrastructure Survey (CIS) is a no-cost, voluntary survey that evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and overall resilience.</td>
</tr>
<tr>
<td>RESPOND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RECOVER</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
For more information about the CSA Program, to schedule a review or assessment, email cyberadvisor@hq.dhs.gov
• 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 by DHS.

For more information, see https://www.cisecurity.org/ei-isac
**EI-GCC Supported Resources**

- Election Infrastructure Security Funding Considerations
- Election Infrastructure Communications Protocol
- Belfer Center Defending Digital Democracy Project (D3P) Playbooks
  - The State and Local Election Cybersecurity Playbook
  - Election Cybersecurity Incident Communication Coordination Guide
  - Election Cyber Incident Communication Plan Template
  - Cybersecurity Campaign Playbook
- Center for Internet Security’s A Handbook for Elections Infrastructure Security
- Private/Non-profit Resources for SLTT & Campaigns
Funding Resources
Most of the updated equipment purchased with HAVA grants are now reaching 10, or in some cases, 14+ years of age.

As of September 30, 2017, states reported that less than 9 percent remain unspent ($323 million in funds and accrued interest).

14 states have expended 100% of their HAVA funds and interest.

29 additional states have less than 10% of HAVA funds remaining.
2018 HAVA Funds

$380,000,000 in Consolidated Appropriation Act, 2018

- Congressional Bill Signed by President Trump - March 22, 2018
- Titled: ELECTION REFORM PROGRAM
- Under HAVA SECTION 101
- Funds must be expended by March 22, 2023
• States were required to submit a 2-3 page narrative overview of activities supported with the funds and a line item budget.
• As of Monday, August 27, the EAC had received narratives and budgets from 50 out of the 55 eligible states and territories.
• 96 percent of the funds have been disbursed.
• Remaining 4 percent still await state resolution of administrative issues related to their U.S. Treasury accounts.
• States must match 5 percent of the federal funds.
State-by-State Breakdown

Amongs:
- $7.9 - $34.6 million
- $5.2 - $7.8 million
- $3.1 - $5.1 million
- $600K - $3.0 million

State has requested funds

Revised on July 16, 2018 - 10:00 am
# How States Plan to Use 2018 HAVA Funds

<table>
<thead>
<tr>
<th>Cybersecurity</th>
<th>Voting Equipment</th>
<th>Reserve</th>
<th>Voter Registration</th>
<th>Election Audits</th>
<th>Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>AL IA NE SC WY</td>
<td>AK HI NM VT AR ID OK WV AS KY PA WY CA LA RI CO MA SC CT MD SD DC MO TN DE ND TX GA NE UT GU NJ VA</td>
<td>AS MS VA CA NE VI CO NH WA FL NJ GU NM HI NV IA OR ID PR MI RI MN TX</td>
<td>AL ID NV AS IN OH AZ MA OK CA ME PR CO MI RI CT MO TN DC NC TX GU NE VI HI NJ UT IA NM WA</td>
<td>AL MI VA CA MN VT CO NC WA CT NJ GA NV GU OH IA OR ID RI KY TX MD UT</td>
<td>AS MI CO NE CT NJ DC NV FL VA GU VI IA WV ID IN MD</td>
</tr>
</tbody>
</table>
Best Practices
Voting System Best Practices

1. Voting systems must produce a voter-verifiable auditable record.
2. Election officials must conduct audits.
   - Statistically sound, efficient audits of the outcome of the elections
   - Audits of the voting system software
3. Ensure that all aspects of voting system (VS, EMS, Ballot Creation) are not connected to internet; use clean media & air gaps.
Election Infrastructure Security – Best Practices

1. Assess your data risks & secure it appropriately
2. Continuous monitoring
3. Develop an incident response & recovery plan
4. Conduct trainings and exercises
5. Take advantage of all available resources
Contact

Geoff Jenista
Cyber Security Advisor
Department of Homeland Security
Geoffrey.jenista@hq.dhs.gov
(913) 249-1539

Ryan Macias
Senior Election Technology Specialist
U.S. Election Assistance Commission
rmacias@eac.gov
(202) 579-5496