2016 Attack & Aftermath
6/23/16
• Attack begins

7/12/16
• Attack escalates
• Deadlocks database
• SBE discovers vulnerability and patches it

7/13/16
• SBE continues analysis of attack
• SBE takes IVRS and associated applications offline

7/19/16
• SBE notifies General Assembly of breach

7/21/16
• SBE begins bringing IVRS back online

7/28/16
• All systems back to full functionality
Post-Attack Activities

• Notified ~76,000 voters in accordance with Illinois privacy laws
• Began working with the FBI in August 2016; Evidence handoff complete in October 2016
• DHS’s US Computer Emergency Readiness Team (US-CERT) confirms that there is no ongoing malicious activity in SBE systems
• Developed an online tool to inform affected voters of the specific information in their voter record
Post-2016 Improvements

• Hired a Full-time Information Security professional
• Send logs from all servers & network devices to DoIT’s Security Operations Center (SOC)
• Deployed full suite of Next Generation Endpoint Security products
• Conducting ongoing penetration tests and internal authenticated vulnerability scans
• Instituted security-first development methodology with multiple automated controls to prevent common vulnerabilities
The SBE - 2016 vs. 2019

2016
• No security partnership with DoIT
• No full-time infosec staff
• No staff security training
• Operations > Security
• No involvement in external Elections security organizations
• No security framework

2019
• DoIT provides SOC monitoring, vulnerability scans, penetration testing
• Full-time infosec professional
• All staff required to complete annual security awareness training
• Security = Operations
• Membership in MS-ISAC, EI-ISAC
• Aligned to CIS Controls
2018 HAVA Election Security Grant Funds
March 2018 – The US Election Assistance Commission (EAC) announced the appropriation of $380 million for election security.

Illinois was awarded $13,232,290 with a non-Federal match requirement of $661,615 (5%) for a total of $13,893,905.

The stated purpose of the funds: To assist your state with activities to improve the administration of elections for Federal office, including by enhancing election technology and making security improvements.
• The FY19 Budget Implementation Bill signed on June 4th includes the following amendment:

  • Sec. 1A-55. Cyber security efforts. The State Board of Elections shall provide by rule, after at least 2 public hearings of the Board and in consultation with the election authorities, a Cyber Navigator Program to support the efforts of election authorities to defend against cyber breaches and detect and recover from cyber-attacks. The rules shall include the Board's plan to allocate any resources received in accordance with the Help America Vote Act and provide that no less than half of any such funds received shall be allocated to the Cyber Navigator Program. The Cyber Navigator Program should be designed to provide equal support to all election authorities, with allowable modifications based on need. The remaining half of the Help America Vote Act funds shall be distributed as the State Board of Elections may determine, but no grants may be made to election authorities that do not participate in the Cyber Navigator Program.
Financial Particulars

• First expenditure was in September of 2018.
• Have spent approximately $1.8 million on the CNP so far. Anticipate spending $3.5 million per year over the next 3.5 fiscal years.
• This depends on the local election officials’ needs and requests. $2.9 million was made available for use by the LEOs in September of 2018.
• Approximately $468,000 has been requested so far.
• Grant ends in March of 2023.
What does Sec. 1A-55 do?

- Creates the “Cyber Navigator Program”
  - An effort to help election authorities to defend against, detect, and recover from cyberattacks
- Directs the SBE to provide equal support to all Illinois Election Authorities (with allowable modifications based on need)
- Directs the use of 2018 HAVA Election Security Grant Funds
  - Half ($6,946,952.50) must to go the Cyber Navigator Program
  - Half ($6,946,952.50) may be used at the SBE’s discretion
  - No grants from the security funds may be made to election authorities that do not participate in the CNP
The Cyber Navigator Program
Defend, Detect, & Recover
# Cyber Navigator Program Components

<table>
<thead>
<tr>
<th>Element</th>
<th>Program Component</th>
<th>Responsible Entity(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure</td>
<td>IVRS Secure Network via the Illinois Century Network (ICN)</td>
<td>DoIT ICN</td>
</tr>
<tr>
<td>Information Sharing, Incident Reporting, and Threat Intelligence</td>
<td>Cybersecurity Information Sharing Program (CISP)</td>
<td>SBE, ISP STIC</td>
</tr>
<tr>
<td>Personnel</td>
<td>Cyber Navigators</td>
<td>DoIT Information Security</td>
</tr>
</tbody>
</table>
Infrastructure – Illinois Century Network (ICN)

• High performance network built to meet the Internet and Intranet needs of the educational, research, governmental, and healthcare organizations serving the state of Illinois
• Serves as an Illinois “local area network”
• Maintained by the Illinois Department of Innovation & Technology (DoIT)
• Distributed Denial of Service (DDoS) Mitigation
• Cleaner, safer internet through IP filtering, geo-filtering, etc.
• Election Authorities keep and maintain complete control over their perimeter firewalls
• All transfer of voter information and access to IVRS will occur on a private network and not over the internet

Confidential/FOUO
Information Sharing - Cybersecurity Information Sharing Program

• Maintain relationships with election officials throughout Illinois
• Disseminate information on cybersecurity “best practices”
• Facilitate the flow of threat intelligence between local election officials and State/Federal partners
• Conduct webinars and conferences focused on cybersecurity
• Oversee security awareness training for local election officials and their staffs
• Work with local election officials to ensure that they have access to all available services and assistance in the event of a cyberattack
• Provide routine administrative updates to the State Board of Elections
Personnel – Cyber Navigators

- Staffing – 9 Navigators (1 Lead Navigator)
- Perform Risk Assessments and present materials to local EAs
- Present risk assessment results to EAs and provide guidance on mitigating the findings
- Establish ICN Connections for EA connectivity to IVRS
Cyber Navigator
Regional Assignments

- 2 Navigators for each zone
  - Zone 1 – Carbondale & Effingham
  - Zone 2 – Springfield & Peoria
  - Zone 3 – Champaign & Taylorville
  - Zone 4 – Chicago & Rockford
• Risk Assessments of Election Authority physical security
• Risk Assessments of Election Authority Election equipment
• Additional Services will be offered as part of the program
• Proactive Phishing Campaigns
• Phishing and Security Training Courses
• Internet Access with IPS and IDS Protection (Clean Internet)
• MS-ISAC Albert Intrusion Detection and Alerting
• SIEM Log Collection and Monitoring by DoIT SOC
• Vulnerability Scans of EA Systems
• External Penetration Testing
Election Threat Planning

Planning, Communication, Incident Reporting
State & Federal Partnerships

- Illinois Department of Innovation & Technology (DOIT)
- Statewide Terrorism & Intelligence Center (STIC)
- Department of Homeland Security (DHS)
- Multi-State Information Sharing & Analysis Center (MS-ISAC)
- Illinois State Board of Elections (SEALS)
- Illinois State Police (ISP)
- Illinois National Guard (ING)
Tabletop Exercises (TTXs) & Training

• **July 2019** – Regional TTX for all 4 zones.

• **April 2019** - National Guard, SBE Staff, and DoIT Infosec staff participated in National Cyber Shield exercise in Indianapolis.

• **October 30, 2018** – Pre-Election Tabletop Exercise between SBE, DoIT, STIC, and the ILNG to simulate Election Day reporting, intelligence flow, communication, and response scenarios.

• **August 14, 2018** – DHS Tabletop the Vote TTX hosted by DHS for state election officials around the country. The SBE invited members of the County Clerk Advisory Committee, DHS, ILNG, DoIT, and STIC.

• **June 21-22, 2018** – Cybersecurity Conference in Bloomington hosted by Illinois Association of County Clerks and Recorders open to all Illinois Election Officials.
Incident Reporting on Election Day

Local/State Incident Identified → Contact STIC

Illinois Election Room
- Homeland Security Information Network (HSIN)

STIC Notifies Partners
- DHS
- FBI
- MS/EI-ISAC
- DoIT/ILNG
2020 General Election

Situational Awareness
- HSIN Connect Virtual Situation Room
- SBE, DoIT, FBI, DHS, MS-ISAC, EI-ISAC, STIC, National Guard
- Status calls held at 11am & 7pm

Monitoring
- DoIT Security Operations Center Staff
- Monitoring Network
- Supplemented by National Guard
- Albert appliance monitoring at Federal level

Incident Response
- IL National Guard Activated and standing ready
- Cyber Navigators on site