CIS Election Security Best Practices

2019 Update

Phyllis Lee, Sr. Director of CIS Controls

NIST Information Security and Privacy Board, December 5, 2019
Agenda
Election Security Best Practices

• Part of the CIS Controls team

• Team
  – Aaron Wilson, Senior Director of Election Security
    • Former FL Election Official
    • Former Election Technology Product Director
  – Mike Garcia, Senior Advisor for Elections Best Practices
    • Former NIST Lead of Trusted Identities Group
    • Former DHS Senior Cyber Security Strategist
CIS Controls Introduction

- Globally recognized cybersecurity standard
- Over 200,000 downloads since CIS took the reigns
- 20 top-level controls followed by 171 sub-controls
- Prioritized set of actions that’s designed to scale
- Provides a logical path to build a foundation and gradually improve your cybersecurity posture
- Version 7.1 released in April 2019
- *Developed by cybersecurity experts*
Election Security Best Practice Guidance

- Election Infrastructure Assessments (2019)
- Security in Election Technology Procurements (2019)
- Election Infrastructure Supply Chain Guidance (2020)
- Election Benchmarks (2020)


www.cisecurity.org/elections-resources
Election Infrastructure Security Handbook

• Release Feb 2018, v2 coming in 2020
• 88 best practices
  – Users
  – Processes
  – Devices
  – Software
  – Transmission
• Mapped to the CIS Controls
• Nearly 20,000 downloads of the handbook, over 5,000 of the excel version
Election Infrastructure Assessment Tool (EIAT)

- Web-based security self-assessment platform
- Based on *A Handbook for Election Infrastructure Security*
- Assesses 88 best practices against
  - voter registration systems,
  - pollbooks,
  - state and local election management systems,
  - vote capture,
  - vote tabulation, and
  - results publishing systems
- Usable by both state and local election offices
EIAT Community

- Over 604 users representing 34 states and 265 local election jurisdictions
- Working directly with:
  - New York
  - Florida
  - Virginia
  - Michigan
  - Idaho
  - California
Election Security Self-Assessment Program

• 6 Step Process
• Supported by EIAT
• Based on Handbook
• Video Training

https://www.cisecurity.org/elections-resources/election-security-self-assessments/
Procurement Guidance

- Qualifications and Experience
- Policies, Procedures and Performance Standards
- Leadership and Personnel Plan
- Risk Management and Incident Response
- Data Management and Handling
- Security Policies, Planning, and Practices
- Supply Chain Approach
- Access Controls
- System Architecture and Cryptography

Category
- People
- Process
- Technology

System Applicability
- All
- Operational
- Critical

IT Type
- Hardware
- Software
- Services
- Cloud
Election Technology Procurements

• Suggested Language
• Good Response
• Bad Response
• Tips
Web Based Search and Export

Security in Election Procurements – Best Practices Search

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
<th>Category</th>
<th>System Applicability</th>
<th>IT Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Qualifications and experience of individuals proposed for work.</td>
<td>People</td>
<td>All</td>
<td>Hardware Services</td>
</tr>
<tr>
<td>2</td>
<td>Demonstrated past performance performing proposed work. Includes awareness of, and experience adhering to, applicable certifications and legal and regulatory requirements.</td>
<td>People</td>
<td>All</td>
<td>Hardware Services</td>
</tr>
<tr>
<td>3</td>
<td>Proposer personnel policies regarding hiring and conduct standards, including background check, citizenship, and visa requirements.</td>
<td>People</td>
<td>All</td>
<td>Hardware Services</td>
</tr>
</tbody>
</table>
Non-Voting Election Technology Best Practices

- Exposure to more threats
- Significant impact on voter confidence
- Covers an existing gap
- Target audience is technology providers
Structure

Technology Areas
- Background
- Threats
- Governance

Best Practices
- Description
- Election
- Technology
- Application

Recommendations
- Technical
- Description
- Election Notes
Organization and Structure

- Technology Areas
- Profile Levels

Diagram: 
- Users
- Administrators
- Software Applications
- Servers & Workstations
- Networking & Architecture
- Data
- Administration
Content

• Hosting and Architecture
  – 1.1 Boundary Defense
  – 1.2 Limitation and Controls of Network Ports, Protocols, and Services
  – 1.3 Secure Configuration for Network Devices
  – 1.4 Data Recovery Capabilities
  – 1.5 Denial of Service Protections
  – 1.6 Wireless Access Control

  ▪ Servers and Workstations
    ▪ 2.1 Secure Configuration for Hardware and Software on Mobile Devices
    ▪ 2.2 Continuous Vulnerability Management
    ▪ 2.3 Malware Defenses
    ▪ 2.4 Controlled Use of Administrative Privileges
    ▪ 2.5 Handling Removable Media

  ▪ Software Applications
    ▪ 3.1 Secure Programming
    ▪ 3.2 Application Development

▪ Data
  ▪ 4.1 Data Protections
  ▪ 4.2 Controlled Access Based on Least Privilege
  ▪ 4.3 Cloud Storage Configuration

▪ Administration
  ▪ 5.1 Account Monitoring and Control
  ▪ 5.2 Implement a Security Awareness and Training Program
  ▪ 5.3 Maintenance, Monitoring, and Analysis of Audit Logs
  ▪ 5.4 Incident Response and Management
Denial of Service Example

1. Deny Communications with Known Malicious IP Addresses
   1.3.4 - Install the Latest Stable Version of Any Security-Related Updates on All Network Devices
   1.5.1 - Establish and Maintain Effective Partnerships With Your Upstream Network Service Provider
   1.5.2 - Port and Packet Size Filtering
   1.5.7 - Set Up Out-of-Band Communication for DDoS Response

2. Enable Firewall Logging
   1.5.5 - Configure Devices to Detect and Alarm on Traffic Anomalies
   5.4.2 - Assign Job Titles and Duties for Incident Response

3. Configure Perimeter Devices to Prevent Common Types of Attacks
   1.5.6 - Establish DDoS Mitigation Services With a Third-Party DDoS Mitigation Provider
   3.2.12 - Deploy Web Application Firewalls
## Ransomware Example

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 1 | 1.1.4 Deny Communications with Known Malicious IP Addresses  
  1.1.6 Deploy Network-Based IDS Sensors  
  1.4.1 Ensure Regular Automated Backups  
  1.4.2 Perform Complete System Backups  
  1.4.4 Protect Backups  
  1.4.5 Ensure All Backups Have at Least One Offline Backup Destination  
  2.3.1 Utilize Centrally Managed Anti-Malware Software  
  4.1.1 Maintain an Inventory of Sensitive Information  
  4.1.2 Remove Sensitive Data or Systems Not Regularly Accessed by the Organization |
| 2 | 1.4.3 Verify Data on Backup Media  
  1.1.7 Deploy Network-Based Intrusion Prevention Systems  
  2.3.3 Enable Operating System Anti-Exploitation Features and Deploy Anti-Exploit Technologies  
  2.4.3 Ensure the Use of Dedicated Administrative Accounts  
  4.2.5 Segment the Network Based on Sensitivity |
| 3 | 1.1.2 Scan for Unauthorized Connections across Trusted Network Boundaries  
  1.4.6 Verify Complete System Recovery  
  2.3.7 Deploy a Host-Based Intrusion Detection System  
  4.1.4 Monitor and Detect Any Unauthorized Use of Encryption |
Non-Voting Election Technology Verification

- Developing new process for verification called RABET-V
  - Rapid Architecture Based Election Technology Verification

- Workshop, November 2019
  - 43 participants representing state and local election jurisdictions, election technology providers, voting system test labs, independent election organizations, and federal government entities including the EAC, NIST, and DHS.

- 2020 Pilot Program
RABET-V Motivations

- Produce a high confidence and more rapid, less expensive process for verifying non-voting elections systems
- Allow for product changes in a quick and cost-effective way (i.e. change tolerance)
- Align verification of election systems with modern software development, testing, and deployment practices
- Provide evidence-based assurance of system reliability and security (using evidence from developers to the extent possible)
- Build on experience of similar industries, such as the medical device industry
• **Pre-Market Review:** Make risk-based testing decisions about product changes based on the
  – Robustness of the system’s architecture
  – Maturity of the provider’s processes

• **Post-Market Operation:** Iterative product verification process is product specific
  – Testing methods used vary based on risk and size/scope of the change
RABET-V Security Claims

• Provides a way to verify rapidly changing technology
• Works with smaller, more frequent releases which provide more opportunity for security patching
• Security patches and non-security impacting changes will be quick to verify
• Encourages better constructed solutions with well-defined architectures
• Encourages usage of well-vetted 3rd party products and packages
• Encourages well-vetted supply chains and change management processes
• Incentivizes internal security testing with automated tools
Election Infrastructure Supply Chain Guidance

- ETA Spring 2020
- Empower election officials and technology providers with action-oriented guidance to reduce supply chain risk
- Distill guidance from NIST and DHS

- Learn
  - Basic background on what supply chains are and how they impact cyber security

- Act
  - What you can do to reduce your supply chain risk
    - Right now
    - When your purchase new products
    - When you receive products
    - When you use products

- Strengthen
  - More resources, in-depth discussion
Election Benchmarks

CIS Benchmarks™

- Windows 10 EMS Gateway (Active)
  - Working with State of Arizona
- Windows 10 EMS
  - Based on Windows 10 IOT
- Microsoft Azure for Elections
- AWS for Elections
Thank You!

Phyllis Lee

electionresources@cisecurity.org