

# CIS Election Security Best Practices

## 2019 Update

Phyllis Lee, Sr. Director of CIS Controls

NIST Information Security and Privacy Board, December 5, 2019


### Election Security Best Practices

- Part of the CIS Controls team
- Team
  - Aaron Wilson, Senior Director of Election Security
  - Samuel H. Mitchell, Chief, Senior Director, Technology Product/Developer
  - Mike Ganga, Senior Advisor for Elections Best Practices
  - Andrew Hill, Chief of Product Operations/Lead Release/CI/CD Senior Cyber Security Strategist



### Election Infrastructure Security Handbook

- Release Feb 2019, v2 coming in 2020
- 88 best practices
  - 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,
  - voter capture,
  - voter tabulation, and
  - results publishing systems
- Usable by both state and local election offices




### 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

### Non-Voting Election Technology Best Practices

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




### Non-Voting Election Technology Verification

- Developing new process for verification called NABET II
  - Repeat Architecture Based Election Technology Verification
- Workshop, November 2018
  - 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

### Election Infrastructure Supply Chain Guidance

- ETX Spring 2020
- Empower election officials and technology providers with action-oriented guidance to reduce supply chain risk
- Draft guidance from NIST and DHS
- Learn
  - Team background on what they, DHS, and NIST did to reduce their election system security
- Ask
  - What else can we do to reduce our election system risk
  - Right now
  - Right later
  - What are the critical next steps
  - What are the critical next steps
  - What are the critical next steps
- Next Steps
  - Share resources in depth discussion

### Election Benchmarks



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

### Thank You!

Phyllis Lee  
[electionresources@cisecurity.org](mailto:electionresources@cisecurity.org)



# 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



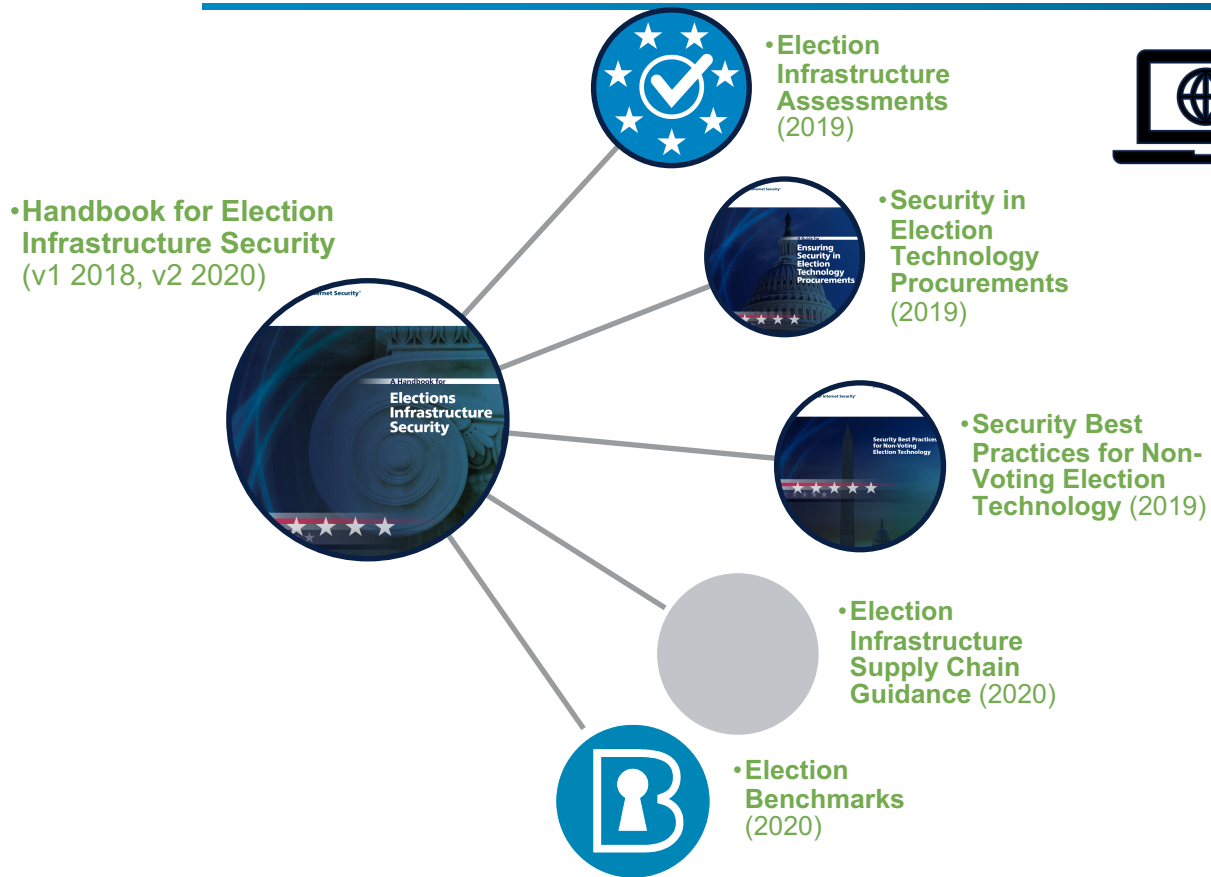


# CIS Controls Introduction

---

- 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



[www.cisecurity.org/elections-resources](http://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

• Whitelist which IPs can access the device [Network Connected]

	Policy Defined	Status	Connected Class	Priority
Voter Registration	Policy Defined	Not Implemented	Network Connected	High
Results Publishing	Policy Defined	Partially Implemented		
User Notes		Implemented In Some Components	Initial Costs	On-going maintenance
		Fully Implemented	Low	Low
		Not Applicable		

Save Response  
 Flag for further review

**Description** CIS Control and Guidance Top Resources

For each type of device (e.g. pollbook, vote tabulation, workstations, routers), determine what other devices require access to it and individually open access to each device by "whitelisting," or explicitly allowing access, each connecting device's IP address. This is to ensure that the connecting device has similarly gone through a whitelisting process and can be trusted. Whitelisting also prevents unknown devices from accessing the network. Start by denying all connections to the device and, as other devices go through a similar whitelisting process and require connection with each other, create connection rules between devices.

Whitelisting is almost never enabled by default, therefore, a specific effort must be made to ensure all devices have whitelisting rules applied.

**Recommendations**

- Ensure all potentially-connected devices have static IP addresses
- Configure the firewalls to block all incoming and outgoing connections





# 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/>

## 6 Steps for Performing Election Security Self-assessments

Understanding your risks is key to a strong cyber defense. When was the last time your elections agency conducted an election security assessment to understand risks? CIS has developed the Election Infrastructure Assessment Tool (EIAT), a program to help your agency conduct an election security self-assessment.

→Related videos and resources

The EIAT is intended to help organizations assess current cyber defenses and make a plan to remediate security vulnerabilities. The tool should also foster awareness building among key stakeholders in security processes. It all comes from conducting a robust assessment. Keep reading for key steps to performing an election security self-assessment for your organization.

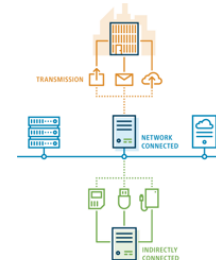
### 1 Step 1: Engage Stakeholders

As an election official charged with a multitude of responsibilities, there are a number of resources available to assist you. As you embark on your self-assessment, engage your jurisdiction's IT administrators to assist and make sure your efforts align with county policies. Leverage your professional associations to share experiences and expertise. Reach out to your vendors to gain their insight on the aspects of the system they cover. This type of feedback will help structure your approach and reduce any apprehension.

### 2 Step 2: Gather Information and Complete the Assessment

The EIAT classifies best practices based on the class of connectedness. These classes consist of network-connected, indirectly connected, and transmission (see Figure 1).

You should first assess your inventory of systems and devices, including those dedicated to the election process, to determine which network connected class they fall into. Use the EIAT to review each of the best practices to find out if the best practice is implemented, has policy defined, or, perhaps, is not applicable.



### 3 Step 3: Review Results

Once complete, the EIAT will provide an overall report based on your self-assessment. Using these results, discuss the findings with your key stakeholders to determine what changes may need to be considered and what the findings mean. You may also find that some of the evaluation findings need to be revisited based on the initial assessment.

### 4 Step 4: Make a Remediation Plan

The review of your results should become your remediation plan. It may include small changes and substantial process or technical changes that involve other departments across your jurisdiction. The EIAT findings and dashboard provide a key tool to brief other senior leaders on the need to take action, whether that involves policy shifts or budget requests to improve your overall security. Use it to establish clear milestones for achieving your goals. The EIAT will provide helpful recommendations on how to take immediate action to boost your score in the dashboard.

### 5 Step 5: Follow your Remediation Plan

Based on your results, establish your milestones and stick with them. This goes back to engaging stakeholders early and throughout the process. With strong and continual engagement, others are more likely to remain committed to seeing full implementation of best practices.

### 6 Step 6: Repeat

Self-assessments are only the first step. Security threats constantly evolve just as fast as technology. Due-diligence requires dedication to a program structure that revisits the EIAT after each election to review the latest best practices and retool.



## Category

- People
- Process
- Technology

## System Applicability

- All
- Operational
- Critical

## IT Type

- Hardware
- Software
- Services
- Cloud

- **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**

# Election Technology Procurements

- Suggested Language
- Good Response
- Bad Response
- Tips

A Guide for Ensuring Security in Election Technology Procurements

44

Part VI: Best Practices for Cybersecurity in IT Procurement

---

<p><b>Practice: #27</b> Use of open standards and common approaches in software and common data formats.</p>	<p><b>System applicability:</b></p> <ul style="list-style-type: none"> <li>• All</li> </ul>	<p><b>IT type:</b></p> <ul style="list-style-type: none"> <li>• Software</li> </ul>
--	---	---

---

**Suggested language:**

- For user- and client-specific software and applications, confirm on which types of systems and, where applicable, browsers the product will have full functionality. In general, products should be fully functional on a host of systems, to include notebooks (such as Chromebooks) and all major browsers.
- If managing voter or ballot data, provide the data format(s) you are using and identify common functions supported with those formats (e.g., risk-limiting audits).

---

**Good:**  
Applicable products are fully functional across a host of systems and browsers or, if not, a full description is provided as to why this is not possible.

---

**Bad:**  
A lack of planning or formalized decision around the approach. Support only for specific browsers or systems that don't represent the whole of your environment.

---

**Tips:**

- Development toward specific systems—even if they are the only systems you have in your environment—is generally frowned upon. This goes beyond compatibility; if something is developed in such a way that it only functions on a specific system, this may indicate that the proposer is not using the most common, and thus best-vetted, standards.
- While it is good to have flexibility to work across multiple versions of a browser, it should be expected that the software will be maintained to use the most current or very recent versions and have a policy of deprecating older versions that are no longer secure.
- Security audit functions are typically performed outside of the system and thus it is important that systems make data available for auditing in common formats that meet the auditing needs of the election officials.

---

**References and links:**

- NIST SP 1500-100 Election Results Common Data Format:  
<https://www.nist.gov/it/voiting/interoperability/election-results-reporting-cdf>



# Web Based Search and Export



Confidence in the Connected World

Quick Links:

[CIS Controls](#) [CIS Benchmarks](#) [CIS Hardened Images](#) [ISAC Info](#)

**CIS SecureSuite<sup>®</sup>**  
Membership

[Apply](#) [Learn more](#) [Login](#)

Cybersecurity Best Practices

Cybersecurity Tools

Cybersecurity Threats

Home • Elections Resources • Security in Election Procurements – Best Practices Search

## Security in Election Procurements – Best Practices Search

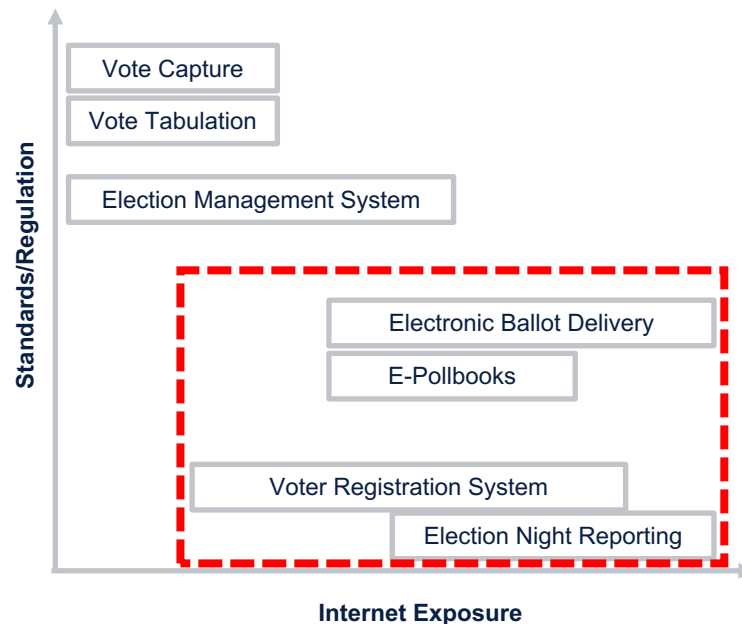
Number	Description	Category	System Applicability	IT Type	<a href="#">View All Best Practices</a>	<a href="#">Export Selected</a>
<input type="text" value="0"/>	<input type="text" value="search"/>	<input checked="" type="checkbox"/> People <input checked="" type="checkbox"/> Process <input checked="" type="checkbox"/> Technology	<input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> Operation <input checked="" type="checkbox"/> Critical	<input checked="" type="checkbox"/> Hardware <input checked="" type="checkbox"/> Software <input checked="" type="checkbox"/> Services <input checked="" type="checkbox"/> Cloud	<a href="#">Update</a>	<a href="#">Uncheck Filters</a>
1	Qualifications and experience of individuals proposed for work.	People	All	Hardware Software Services		
2	Demonstrated past performance performing proposed work. Includes awareness of, and experience adhering to, applicable certifications and legal and regulatory requirements.	People	All	Hardware Software Services Cloud		
3	Proposer personnel policies regarding hiring and conduct standards, including background check, citizenship, and visa requirements.	People	All	Hardware Software Services Cloud		

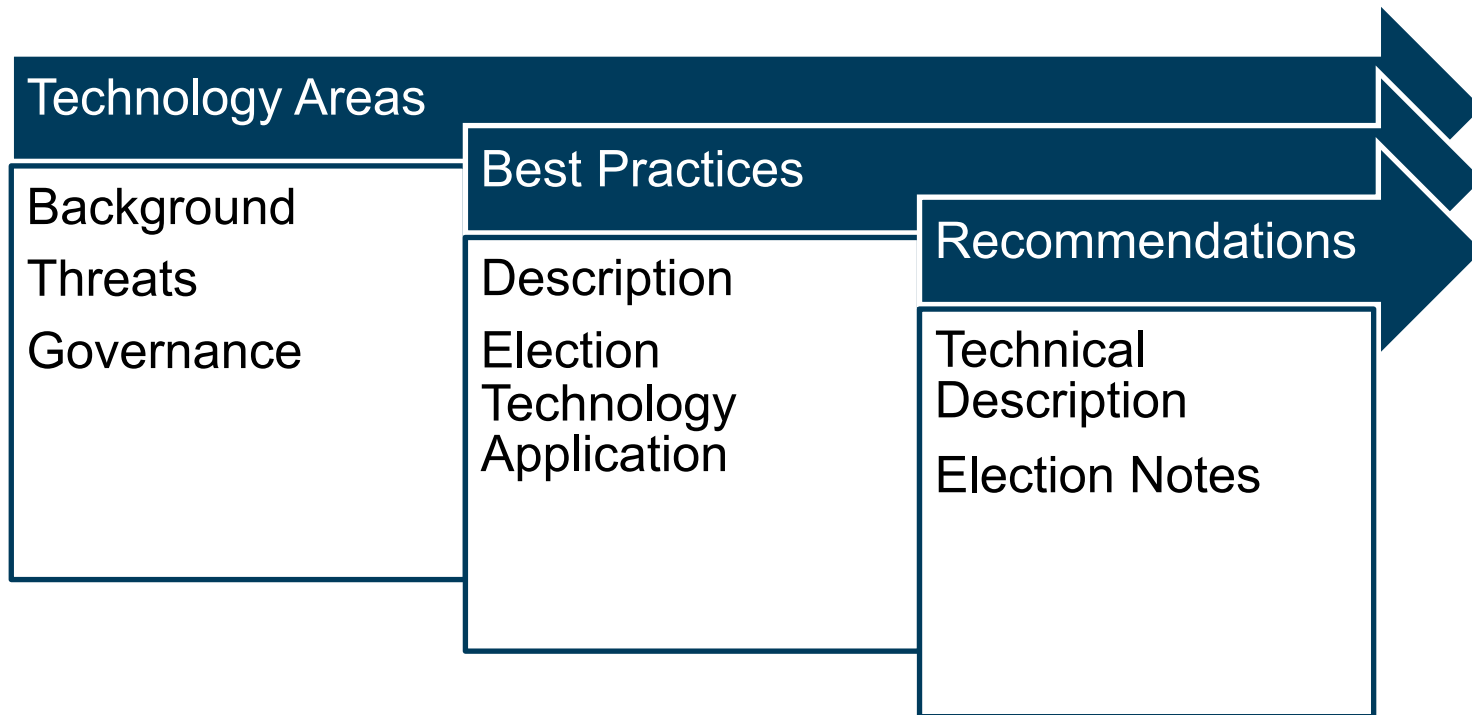
Proposer location(s) where work will be performed

# Non-Voting Election Technology Best Practices



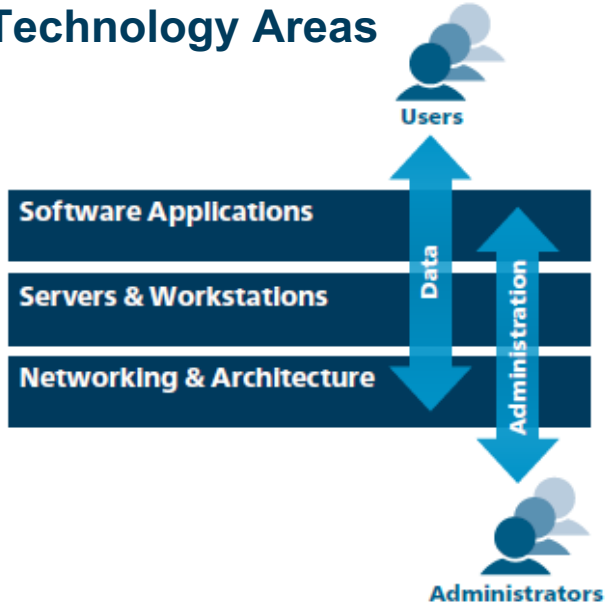
- Exposure to more threats
- Significant impact on voter confidence
- Covers an existing gap
- Target audience is technology providers



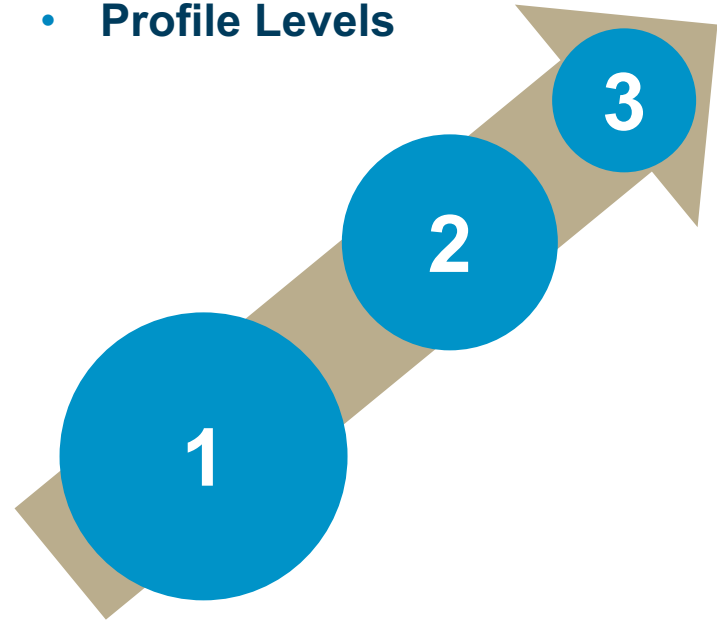


# Organization and Structure

- Technology Areas



- Profile Levels





# 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

1.1.3 - 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

1.5.3 - 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

1.5.4 - 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

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**

# RABET-V Process Framework

Provider Submission



Security Claims Review



Architecture Review	Process Assessment
---------------------	--------------------

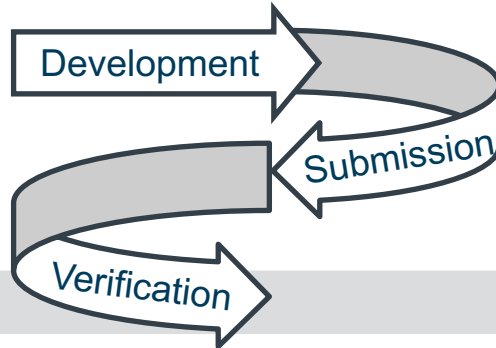


Product Testing Process

Pre-Market Review

Market Operation

- **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 3<sup>rd</sup> 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 you 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](mailto:electionresources@cisecurity.org)**