Principle 14
System Integrity

The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

Requirements for Principle 14Principle 14 System Integrity The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

14.1 - The voting system uses multiple layers of controls to provide redundancy against security failures or vulnerabilities.

14.1-A – Risk assessment documentation
14.1-B – Addressing and accepting risk
14.1-C – System security architecture description
14.1-D – Procedural and operational security

14.2 - The voting system limits its attack surface by reducing unnecessary code, data paths, and physical ports, and by using other technical controls.

14.2-A – Extraneous processes and services
14.2-B – Non-essential features
14.2-C – Network status indicator
14.2-D – Wireless network status indicator
14.2-E – Secure configuration and hardening
14.2-F – Secure configuration and hardening documentation
14.2-G – Unused code
14.2-H – Exploit mitigation technologies within platform
14.2-I – Application use of exploit mitigation technologies
14.2-J – Importing software libraries
14.2-K – Physical port restriction
14.2-L – Known vulnerabilities
14.2-M – List of known vulnerabilities

14.3 - The voting system maintains and verifies the integrity of software, firmware, and other critical components.

14.3-A – Supply chain risk management strategy
14.3-B – Criticality analysis
14.3-C –Bill of Materials
14.3.1 – Boot integrity
14.3.1-A – Cryptographic boot verification
14.3.1-B – Preventing of boot on error

14.3.1-C – Logging of verification failure

14.3.2 – Software integrity

14.3.2-A – Installing software

14.3.2-B – Software verification for installation

14.3.2-C – Software whitelisting

14.3.2-D – Integrity protection for software whitelists

14.4 - Software updates are authorized by an administrator prior to installation.

14.4-A – Authenticated operating system updates

14.4-B – Authenticated application updates

14.4-C – Authenticated firmware updates

14.1 - The voting system uses multiple layers of controls to provide redundancy against security failures or vulnerabilities.

14.1-A – Risk assessment documentation

The voting system's documentation must contain a risk assessment

Discussion

Risk assessments are a foundation of effective risk management. Additionally, they help to facilitate decision making at the organization, business process, and information system levels. Many methods of conducting risk assessments exist, including NIST SP 800-30-1: Guide for Conducting Risk Assessments or ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management.

External references:	NIST SP 800-30-1: Guide for Conducting Risk Assessments ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management
Related requirements:	[documentation]

14.1-B – Addressing and accepting risk

The voting system's risk assessment documentation must provide technical controls or a notation showing the acceptance of risk for each documented threat to voting system integrity.

Discussion

Assigning controls or accepting risk is a key part of the risk assessment process.

Related requirements:	[documentation]

14.1-C – System security architecture description

The voting system's risk assessment documentation must describe how physical, technical, and operational controls work together to prevent, mitigate, and respond to attacks on the voting system. This includes the use of:

1. Cryptography
2. Malware protection
3. Firewall access control lists, rules, and configurations
4. System configurations

Discussion

Risk assessments can be large, complicated documents. This requirement ensures that a single narrative exists to explain to election officials and other system owners how the overall security operates for the voting system.

Related requirements: [documentation]

14.1-D – Procedural and operational security

The voting system must document necessary procedural and operational processes that need to occur to ensure integrity of the system.

Discussion

Procedural and operational security processes play a key role in overall system security. If any of these procedures are necessary to ensure system integrity or system security, these practices need to be well documented and explained.

Related requirements: [documentation]

14.2 - The voting system limits its attack surface by reducing unnecessary code, data paths, and physical ports, and by using other technical controls.

14.2-A – Extraneous processes and services

The voting system must prevent extraneous processes and services from being installed or executed.

Discussion

Attack surface mitigation limits the voting system's exposure to malicious activity. The presence of non-essential programs or network services severely increases attack surface. This can include network services, superfluous userspace processes, integrated development environment, and compilers.

14.2-B – Non-essential features

The voting system must disable networking and other features that are non-essential to the function of the voting system by default.

Discussion

When the voting system is booted, networking and other functions are prohibited from running. For instance, networking interfaces such as eth, wlan, and hci should be off.

By disabling features that are non-essential to the voting system, this decreases the attack surface by limiting the functionality and decreasing the entry points that may be accessed by unauthorized users.

14.2-C – Network status indicator

The voting system application must visually show an indicator within the management interface when networking functionality is enabled and disabled.

Discussion

This helps to ensure that network functionality is not enabled by accident.

14.2-D – Wireless network status indicator

If a voting system has network functionality, the voting system application must visually show an indicator within the management interface when wireless networking functionality is enabled and disabled.

Discussion

Note that this is in addition to the networking identifier.

Wireless is a significant avenue for system compromise. This indicator ensures that wireless functionality is not enabled by accident.

14.2-E – Secure configuration and hardening

The voting system must follow a secure configuration guide for all underlying operating systems and other voting system components, with any deviations from best practice documented and justified.

Discussion
Properly configuring an operating system is a difficult and complex task, with small settings potentially causing a large impact. Industry, NIST, and various agencies within the DoD offer guidance for specific operating systems, as do OS and component manufacturers.

Documenting deviations ensures that important settings are not overlooked and decisions to deviate are properly considered.

14.2-F – Secure configuration and hardening documentation

The voting system documentation must include the guidance used to securely configure the voting system

Discussion
Access to the guidance used for secure configuration provides a reference to ensure the voting system is securely configured.

Related requirements:	[documentation]

14.2-G – Unused code

The voting system application must not contain unused, or dead code.

Discussion
An attacker may be able to take advantage of the unused code and introduce software bugs/exploits that can be used to make the voting system vulnerable.

Dead code is source code that can never be executed in a running program. The surrounding code makes it impossible for a section of code to ever be executed [See MITRE CWE-561- **https://cwe.mitre.org/data/definitions/561.html**]. Software with dead code is considered poor quality and reduces maintainability.

External references:	MITRE CWE-561
Applies to:	Voting System Application

14.2-H – Exploit mitigation technologies within platform

The underlying platform of the voting system must provide modern exploit mitigation technologies such as Data Execution Prevention (DEP) and Address Space Layout Randomization(ASLR).

Discussion

DEP and ASLR are commonplace exploit mitigation technologies that can help prevent a variety of vulnerability types, including memory corruption errors like buffer overflows.

14.2-I – Application use of exploit mitigation technologies

The underlying platform of the voting system must make use of the exploit mitigation technologies provided by the underlying system.

Discussion

Applications need to be written and compiled in such a way as to make use of underlying exploit mitigation technologies.

14.2-J – Importing software libraries

The voting system application must not import entire software libraries where individual functions are more practical.

Discussion

Importing entire software libraries significantly increases the attack surface of the software. Importing only the functions needed is a useful attack surface minimization strategy. Not all 3rd party libraries are easily modifiable, making this attack surface reduction strategy impractical.

Applies to:	Voting System Application

14.2-K – Physical port restriction

The voting system must have the capability to restrict access to physical ports that are meant to be used solely by election judges and administrators.

Discussion

Physical port access needs to be restricted when not in use. This requirement is not meant to impede the use of accessible technology.

Related requirements:	Physical Security

14.2-L – Known vulnerabilities

The underlying voting system platform must be free of well-known vulnerabilities before certification, unless otherwise noted by the certification authority.

Discussion

Vulnerability scanning tools can be used to identify known vulnerbailities in software and firmware. The U.S. National Vulnerability Database (NVD) is one resource that can be useful for identifying known vulnerabilities. Other vulnerability databases also exist and can be leveraged for full vulnerability coverage that might not be identified by automated scanning tools.

14.2-M – List of known vulnerabilities

If the certification authority allows certification of the voting system with known vulnerabilities, a list of these vulnerabilities must be provided to the certification authority before it is certified.

Discussion

Certain information can also be included for each vulnerability, such as any severity, impact, or exploitability scores.

14.3 - The voting system maintains and verifies the integrity of software, firmware, and other critical components.

14.3-A – Supply chain risk management strategy

The voting system's documentation must contain a supply chain risk management strategy that at minimum includes the following:

1. A reference to the template or standard used, if any, to develop the supply chain risk management strategy
2. Identification and prioritization of the critical systems, components and services
3. The contract language that requires suppliers and partners to provide the appropriate information to meet the assurance requirements of the supply chain risk management strategy. This includes the products or services acquired from the suppliers/partners and any evidence or artifacts that attest to the required level of assurance.
4. The plan for reviewing and auditing suppliers and partners
5. The response and recovery plan for a supply chain risk incident

Discussion

Supply chain risks may include insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the technology supply chain. These risks are associated with an organization's decreased visibility into, and understanding of, how the technology that they acquire is developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services. These risks can be managed by…

- Following Appendix E of NIST SP 800-161 – Supply Chain Risk Management Practices for Federal Information Systems and Organizations guidance, Appendix E provides a supply chain management plan(strategy) template.
- Utilizing the NIST Cybersecurity Framework version 1.1. by referencing the Supply Chain Risk Management category and subcategory
- Referencing the relevant security controls for supply chain in NIST SP 800-53 Rev. 5 *Security and Privacy Controls for Information Systems and Organizations*

External references:	NIST SP 800-161 – Supply Chain Risk Management Practices for Federal Information Systems and Organizations NIST Cybersecurity Framework Version 1.1 NIST SP 800-53 Rev. 5

14.3-B – Criticality analysis

The voting system's documentation must include a list of critical components defined by a criticality analysis.

Discussion

Defining the critical components of the voting system can assist in prioritizing their importance to the voting process and identifying the impact to security, privacy and performance for failure or compromise.

This can be supplemented by following NISTIR 8179 *Criticality Analysis Process Model - Prioritizing Systems and Components.*

External references:	NISTIR 8179 – Criticality Analysis Process Model – Prioritizing Systems and Components

14.3-B.1 –Bill of Materials

The voting system's documentation must include the hardware and software information for the critical components defined in the 14.3-B and at minimum list the following information for each component:

1. Component name
2. Manufacturer
3. Model or Version
4. Applicable platform for software (e.g., Windows or Linux)

Discussion

This requirement will use the critical components defined in the critical analysis of 14.3-B.
This is a common practice when providing a hardware bill of materials. It is not as common to produce a bill of materials for software and as standards/best practices are developed, they should be considered for inclusion in the software bill of materials.

External references:	SAFECode - Security Risks Inherent in the Use of Third-party Components

14.3.1 – Boot integrity

14.3.1-A – Cryptographic boot verification

The voting system must cryptographically verify system integrity before the operating system is loaded into memory.

Discussion
This requirement does not mandate hardware support. This requirement could be met by trusted boot, but other software-based solutions exist. This includes a software bootloader cryptographically verifying the OS prior to execution. Verifying the bootloader itself is excluded from this requirement, but not prohibited.

Applies to: Vote capture and tabulation device, EMS

14.3.1-B – Preventing of boot on error

If the voting system fails boot validation, the voting system must not boot and provide an onscreen alert.

Discussion
System users need to be notified when the voting system is either corrupted or has been maliciously modified.

Boot validation prevents unauthorized operating systems and software from being installed or run on a system.

Applies to: Vote capture and tabulation device, EMS

14.3.1-C – Logging of verification failure

The voting system must log if the voting system does not pass boot validation and include any other necessary information to understand the failure.

Discussion
Failure of boot validation needs to be logged so these errors can be further analyzed when needed.

Applies to: Vote capture and tabulation device, EMS

14.3.2 – Software integrity

14.3.2-A – Installing software

The voting system must only allow digitally signed software and firmware to be installed.

Discussion
Signed software and firmware ensures that it is not modified before installation, and that it is being distributed by the proper entity.

14.3.2-B – Software verification for installation

The voting system must cryptographically verify the digital signature of software and firmware before it is installed.

Discussion
The security properties of integrity and authenticity are not achieved unless the digital signature for the signed software and firmware is cryptographically verified.

14.3.2-C – Software whitelisting

The voting system must whitelist all applications running in userspace.

Discussion
This is the principle malware prevention mechanism on the voting system. One method of achieving this is cryptographically verifying the digital signatures of all applications before they are run on the voting system.

Applies to:	Vote Capture Device

14.3.2-D – Integrity protection for software whitelists

The voting system must protect the integrity and authenticity of the whitelist configuration files.

Discussion
If the whitelist is improperly modified, the software whitelisting mitigation can be defeated. The most common way of providing whitelist configuration file protection could be a digital signiature.

Applies to:	Vote Capture Device

14.4 - Software updates are authorized by an administrator prior to installation.

14.4-A – Authenticated operating system updates

The voting system must authenticate administrators before an operating system update is performed.

Discussion
Administrators are required to be authenticated before they can update the voting system, regardless of whether the updated done by a networked method or performed using physical media.

Related requirements:	Access Control
Applies to:	Vote Capture Device

14.4-B – Authenticated application updates

The voting system must authenticate administrators before a software update to the voting system application and related software.

Discussion
Administrators are required to be authenticated before they can update the voting system, whether the update is applied by a network method or physical media.

Related requirements:	Access Control
Applies to:	Vote capture and tabulation device, Network appliances, EMS

14.4-C – Authenticated firmware updates

The voting system must authenticate administrators before a firmware or driver update.

Discussion
Administrators are required to be authenticated before they can update the voting system, regardless if network enabled update is performed or via physical media.

Related requirements:	Access Control
Applies to:	Vote Capture Device