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.

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.

Applies to: Voting system documentation

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. Multiple 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.

Status: New
Updated: Feb 13, 2018
Source: N/A
Gap notes:

14.1-A.1 – Addressing and accepting risk

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

Applies to: Voting system documentation

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

Status: New
Updated: Jan 24, 2018
Source: N/A
Gap notes:

Deleted: A
Deleted: D
Deleted: Voting System Documentation
Deleted: 08
Deleted: Jan
Deleted: 24
Deleted: &
Deleted: A
Deleted: R
Deleted: Voting System Documentation

14.1-A.2 – System security architecture description

The voting system 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:

- Cryptography
- Malware protection
- Firewall access control lists, rules, and configurations
- System configurations

Applies to: Voting system documentation

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 as to how the overall security operates for the voting system.

Status:	New
Updated:	Jan 24, 2018
Source:	N/A
Gap notes:	

14.1-B – Procedural and Operational Security

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

Applies to: Voting system documentation

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.

Status:	New
Updated:	Jan 24, 2018
Source:	N/A
Gap notes:	

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

Deleted: S
Deleted: A
Deleted: D
Deleted: Use of c
Deleted: S
Deleted: D
Deleted: &
Deleted: the system
Deleted:
Deleted: of the voting system
Deleted: Voting System Documentation

14.2-A – Ensuring system integrity

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

Applies to: Voting system

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 may include network services, superfluous userspace processes, integrated development environment, and compilers.

Status: New
Updated: Feb 13, 2018
Source: N/A
Gap notes:

14.2-B – Non-essential services

The voting system must disable networking and other non-essential services by default.

Applies to: Voting system

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.

Status: New
Updated: Feb 13, 2018
Source: N/A
Gap notes:

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.

Applies to: Voting system

Discussion

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

Status: New
Updated: Feb 13, 2018
Source: N/A
Gap notes:

Deleted: S
Deleted: I
Formatted: Indent: Left: 0.25", No bullets or numbering
Deleted: This includes:¶ Network services ¶ Minor userspace processes ¶ IDEs¶ Compilers
Deleted: S
Deleted: (IDE)
Deleted: ts
Deleted: Jan
Deleted: 24
Deleted: Default Settings
Deleted: E
Deleted: S
Deleted: S
Deleted: Upon boot
Deleted: of the voting system
Deleted: must be
Deleted: Jan
Deleted: 24
Deleted: Functionality
Deleted: S
Deleted: I
Deleted: menu
Deleted: S
Deleted: Jan
Deleted: 24

14.2-D – Wireless network status indicator

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

Applies to: Voting system

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.

Status:	New
Updated:	Feb 13, 2018
Source:	N/A
Gap notes:	

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 available guidance.

Applies to: Voting system

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.

Status:	New
Updated:	Feb 13, 2018
Source:	N/A
Gap notes:	

14.2-E.1 – Deviations from secure configurations

Deviations from best practices must be documented and justified.

Applies to: Voting system, Voting system documentation

Discussion

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

Status:	New
Updated:	Jan 24, 2018
Source:	N/A

Deleted: N
Deleted: Functionality
Deleted: S
Deleted: I
Deleted: menu
Deleted: Note: this is in addition to the networking identifier.
Deleted: S
Deleted: Jan
Deleted: 24
Deleted: C
Deleted: &
Deleted: H
Deleted: Guide
Deleted: S
Deleted: Jan
Deleted: 24
Deleted: S
Deleted: C
Deleted: S

Gap notes:

14.2-F – Unused code

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

Applies to: Voting System Application

Discussion

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].

Status: New
Updated: Jan 24, 2018
Source: 2007 VVSG
Gap notes:

14.2-G – 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).

Applies to: Voting System

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.

Status: New
Updated: Jan 24, 2018
Source: N/A
Gap notes:

14.2-H – 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.

Applies to: Voting System

Discussion

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

Status: New
Updated: Jan 24, 2018

Deleted: C

Deleted: }.

Deleted: See CWE-561.

Deleted: M

Deleted: T

Deleted: W

Deleted: P

Formatted: Indent: Left: 0.5", Hanging: 1.5"

Deleted: ¶

Deleted: U

Deleted: E

Deleted: M

Deleted: T

Deleted:

Source: N/A
Gap notes:

14.2-I – Importing software libraries

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

Applies to: Voting System Application

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.

Status: New
Updated: Jan 24, 2018
Source: N/A
Gap notes:

14.2-J – Physical port restriction

The voting system must be able to restrict access to physical ports in a tamper-evident manner.

Applies to: Voting System

Discussion
Physical port access need to be restricted when not in use.

Status: New
Updated: Feb 13, 2018
Source: N/A
Gap notes: Physical Security

14.2-K – Known vulnerabilities

The underlying voting system platform must be free of well-known vulnerabilities.

Applies to: Voting System

Discussion
The U.S. National Vulnerability Database (NVD) is one resource that may be useful for identifying known vulnerabilities. Other databases also exist run by external organizations.

Status: New
Updated: Jan 24, 2018

Deleted: S
Deleted: L
Deleted: P
Deleted: R
Deleted: restrict
Deleted:
Deleted: Jan
Deleted: 24
Deleted: V

Source: N/A
Gap notes:

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

14.3-A – Supply chain

The voting system must provide documentation for all components that are not directly manufactured by the voting system vendor.

Applies to: Voting System

Discussion
Supply chain vulnerabilities may arise when things such as the internal components of the voting system come from an external or foreign manufacturer. These external components may have unknown malware installed which could affect the integrity of the voting system. This can be supplemented by following NIST SP 800-161 – *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* guidance.

Status: New
Updated: Feb 12, 2018
Source: N/A
Gap notes:

14.3-B – Cryptographic boot verification

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

Applies to: Voting System

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.

Status: New
Updated: Jan 24, 2018
Source: N/A
Gap notes:

Deleted: C
Deleted: ,
Formatted: Font: Italic
Formatted: Metadata text
Deleted: A
Deleted: B
Deleted: V

14.3-A .1– Cryptographic verification alert

The voting system must provide an onscreen alert if the voting system does not pass boot validation.

Applies to: Voting System

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

Status: New
Updated: Jan 24, 2018
Source: N/A
Gap notes:

14.3-A.2 – 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.

Applies to: Voting System

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

Status: New
Updated: Jan 24, 2018
Source: N/A
Gap notes:

14.3-B – Software installation

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

Applies to: Voting System

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

Status: New
Updated: Jan 24, 2018
Source: N/A
Gap notes:

Deleted: V
Deleted: A
Deleted: V
Deleted: F
Deleted: ,
Deleted: I

14.3-C – Software verification for installation

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

Applies to: Voting System

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

Status:	New
Updated:	Jan 24, 2018
Source:	N/A
Gap notes:	

Deleted: V

Deleted: I

14.3-D – Software whitelisting

The voting system must whitelist all applications running in userspace.

Applies to: Vote Capture Device

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.

Status:	New
Updated:	Jan 24, 2018
Source:	N/A
Gap notes:	

Deleted: W

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.

Applies to: Vote Capture Device

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

Deleted: OS

Deleted: U

Deleted: if

Deleted: enabled

Deleted: update is

Deleted: or

Deleted: via

Status: New
Updated: Jan 24, 2018
Source:
Gap notes: Access Control

14.4-B – Authenticated application updates

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

Applies to: Voting application

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.

Status: New
Updated: Jan 24, 2018
Source:
Gap notes: Access Control

14.4-C – Authenticated Firmware Updates

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

Applies to: Vote Capture Device

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.

Status: New
Updated: Jan 24, 2018
Source:
Gap notes: Access Control

Deleted: Software
Deleted: U
Deleted: e Capture Device