Communication Security Requirements Gap Analysis

An overarching goal of the next VVSG is to have each requirement mapped to a principle and its associated guidelines. During the mapping activity for the communication security requirements, it was found that some requirements did not map well to the principles and guidelines.

Possible modifications for the communication security requirements and/or guidelines include:

- The NIST team would like to discuss the wireless prohibition with the working group.

  Requirement(s): 5.6.1-A, 5.6.1-B, 5.6.1-B.1, 5.6.1-B.2, 5.6.1-E

- Some requirements may call for the development of a new guideline, which read as follows:

  Access Control
  Voting system devices and network interfaces contain unique identifiers.

  Requirement: 5.6.3-A

  System Integrity
  To the extent possible, the voting system reduces its attack surface through procedural and technical means.

  Requirement: 5.6.3-E, 5.6.3-F

For more information about each requirement, please reference VVSG 2007 at:
http://collaborate.nist.gov/voting/pub/Voting/CyberSecurity/2007-VVSG.pdf

5.6.1-A Prohibiting wireless technology

Requirement:	Electronic devices SHALL NOT be enabled or installed with any wireless technology (e.g., Wi-Fi, wireless broadband, Bluetooth) except for infrared technology when the signal path is shielded to prevent the escape of the signal and saturation jamming of the signal.
Applies to:	Electronic device
Test Reference:	Part 3:4.3 "Verification of Design Requirements"
Discussion:	The transient and mobile properties of wireless networks are more threatening than enabling to the voting process. Wireless interfaces that are inadvertently or purposefully enabled at an electronic device are likely to leave those platforms exposed to attack and exploit, with exfiltration, manipulation, or destruction of data a possible outcome. This requirement supersedes [VVSG2005] I.7.7 by prohibiting usage of wireless technology, except for infrared technology when the physical path is protected, in electronic voting system devices.
Source:	[VVSG2005] I.7.7.1-a-h, I.7.7.2-5

Principle(s)/ Guideline(s):	*Security: Data Protection* The voting system protects sensitive data from unauthorized access, modification, or deletion. **Justification:** This requirement aligns with the Data Protection principle.

5.6.1-B Restricting dependency on public communication networks

Requirement:	Electronic devices SHALL NOT use public communication networks (including, but not limited to the Internet and modem usage through public telephone networks), except for electronic devices at polling places that transmit unofficial end of the day results and interface with voter registration databases on election day.
Applies to:	Electronic device
Test Reference:	Part 3:4.3 "Verification of Design Requirements"
Discussion:	The use of public communications networks would greatly increase the exposure of electronic devices for voting to attack and exploitation. Functions such as software patch distribution may be performed either manually or through a dedicated, standalone network that is not connected to any public communications network. The excepts to this requirement allows for end of day results to be transmitted from a polling place to a central election facility and for activation devices to connect to voter registration databases housed outside of a polling place. This requirement supersedes [VVSG2005] I.7.6 by prohibiting usage of public communication networks for electronic voting system devices.
Source:	[VVSG2005] I.7.6.1, I.7.6.2.1, I.7.6.2.2
Principle(s)/ Guideline(s):	*Security: Data Protection* The voting system protects sensitive data from unauthorized access, modification, or deletion. **Justification:** This requirement aligns with the Data Protection principle.

5.6.1-B.1 Air gap for transmitting end of day results on election day

Requirement:	Electronic devices SHALL NOT be connected to other polling place electronic devices when transmitting end of the day results on election day.
Applies to:	Electronic device
Test Reference:	Part 3:4.3 "Verification of Design Requirements"
Discussion:	This requirement is to provide an air gap between electronic devices networked at the polling place and electronic devices that connect externally from the polling place. This requirement allows for end of day results to be transmitted from a polling place to a central election facility.
Source:	VVSG2007
Principle(s)/ Guideline(s):	*Security: Data Protection* The voting system protects sensitive data from unauthorized access, modification, or deletion. **Justification:** This requirement aligns with the Data Protection principle.

5.6.1-B.2 Air gap for connecting to voter registration databases

Requirement:	Electronic devices that connect to voter registration databases outside a polling place on election day SHALL never be connected to other polling place electronic devices.
Applies to:	Electronic device
Test Reference:	Part 3:4.3 "Verification of Design Requirements"
Discussion:	This requirement is to provide an air gap between electronic devices networked at the polling place and electronic devices that connect externally from the polling place. This requirement allows for activation devices to connect to voter registration databases housed externally from the polling place, but the activation devices cannot be connected to other polling place electronic devices.
Source:	VVSG2007
Principle(s)/ Guideline(s):	*Security: Data Protection* The voting system protects sensitive data from unauthorized access, modification, or deletion. **Justification:** This requirement aligns with the Data Protection principle.

5.6.1-E Implementing unique network identification

Requirement:	Each electronic device SHALL have a unique physical address/identifier for each network interface.
Applies to:	Electronic device
Test Reference:	Part 3:4.3 "Verification of Design Requirements"
Discussion:	Most networking protocols require a unique physical address or other identifier for each network interface so that each network interface attached to a particular network can be uniquely identified. For example, Ethernet requires that each network interface have a unique media access code (MAC) address. Having such an identifier for each network interface is also beneficial for security because it permits each electronic device on a network to be uniquely identified.
Source:	[NIST05] Security Control IA-3
Principle(s)/ Guideline(s):	*General Implementation/Construction:*

5.6.3-A Implementing unique system identifiers

Requirement:	Each electronic device SHALL have a unique system identifier (ID).
Applies to:	Electronic device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	System ID can be in the form of a unique system or device roles that can be used as a mechanism to filter the type of packets that are allowed or dropped by the device.
Source:	[NIST05] Security Control IA-3
Principle(s)/ Guideline(s):	*General: Ease of Evaluation* Ensure reviewers can clearly identify all essential elements of a specified system in evaluated systems – including identification of unique election/auxiliary processes and functions; wherever they are implemented in software, hardware,

	telecom, data, and/or other technology layers of the system; and with an ability to record and track these identifications. **Justification:** Although it tangentially applies, a better guideline may need to be generated.

5.6.3-E Documenting information available to devices

Requirement:	The manufacturer SHALL define the minimum amount of information requested from unauthenticated devices via active network ports and shares.
Applies to:	Electronic device
Test Reference:	Part 1:4.1 "Overview" as part of Requirement Part 1:5.6.3-F
Discussion:	This requirement is meant to document the minimum amount and depth of information available to malicious network entities accessing the electronic device remotely. Information available through banners, help functions, and direct interaction with available ports and shares often gives remote attackers illuminating information about the electronic device. Armed with this expanded information, an attacker can evolve their attack to a more educated and specific effort, increasing probability of a successful attack.
Source:	[SCAM01]
Principle(s)/ Guideline(s):	*Security: Detection and Monitoring* If the voting system contains networking capabilities, it employs appropriate modern defenses against network-based attacks. **Justification:**

5.6.3-F Minimizing information available to devices

Requirement:	Electronic devices SHALL request no more information than required to unauthenticated devices via active network ports and shares.
Applies to:	Electronic device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	This requirement is meant to minimize the amount and depth of information available to malicious network entities accessing the electronic device remotely. Information available through banners, help functions, and direct interaction with available ports and shares often gives remote attackers illuminating information about the electronic device. Armed with this expanded information, an attacker can evolve their attack to a more educated and specific effort, increasing probability of a successful attack.
Source:	[SCAM01]
Principle(s)/ Guideline(s):	*Security: Detection and Monitoring* If the voting system contains networking capabilities, it employs appropriate modern defenses against network-based attacks. **Justification:**