Mapping of VVSG 2007 Communication Security Requirements to VVSG Cybersecurity Working Group Principles and Guidelines

After discussion of the Communication Security Requirements gap analysis (http://collaborate.nist.gov/voting/pub/Voting/CyberSecurity/GapsInCommSecurityRequirements.pdf), the Working Group found these areas for future changes and development to the VVSG communication security requirements include:

- Remove the requirements that disallow the use of wireless technology.

  The initial 2007 VVSG included a ban on all forms of wireless communication, except for infrared technology, as listed in requirement Part 5.6.1-A. The use of wireless could allow malicious entities to sniff the communications channel to obtain sensitive information about the election, such as ballot information, unofficial election results, and system information that could be used to launch a more specific attack. Additionally, the firmware listening on the wireless chipsets themselves could be exploited to provide an attacker system access. Upon assessing the threats associated to the use of wireless in voting systems, the Cybersecurity Working Group believes that the use of software independent voting systems is a strong mitigation for these threats.

  Here is the definition for *wireless technology* to be included in the requirements glossary:

  Wireless Technology is defined as "Technology that permits the transfer of information between separated points without physical connection." (NISTIR 7298 Rev. 2: Glossary of Key Information Security Terms)

- The future cryptography requirements could include the following topics:
  - 802.1x specifications
  - Use of modern network security practices
  - Firewalls/Intrustion Detection and Prevention System
  - Robust password management
  - Network/device whitelisting
  - Robust network protocols

This information below is based on the requirements found at:
http://collaborate.nist.gov/voting/pub/Voting/CyberSecurity/2007-VVSG.pdf

5.6 Communication Security

This chapter provides requirements for communications security. The requirements address both the integrity of transmitted information and protect the voting system from communications based threats. This chapter is organized in three parts. The first set of requirements address physical communication components including the prohibition of radio frequency (RF) capable components. The second set of requirements address data transmission security requirements related to the encoding and decoding data packets, and creating logical paths for transferring data between systems. The third set of requirements address communication security related to the voting application including the authentication of communications between voting devices. Although voting systems can have the capability to communicate with other voting devices, there are key security concerns that must be

accounted for both during voting and when election administrators prepare the voting device. This chapter does not address networking issues based on hand carried electronic media, which are addressed in the Systems Integrity Management Chapter.

5.6.1 Physical communication security

This section describes security requirements for physical communication components of voting systems including the electrical and mechanical hardware that sends and receives data.

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-C Limiting network interfaces based on voting state

Requirement:	Electronic devices SHALL have the ability to enable or disable physical network interfaces (including modems) based upon the voting system state.

Applies to:	Electronic device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Making an electronic device accessible on a network significantly increases the risk of that device to attack and exploitation. Election Officials need the ability to enable a physical network interface for use during a particular voting system state and to disable other network interfaces that are not required during that state. This reduces the exposure of the electronic devices to network-based attacks.
Source:	[NIST05] Security Control AC-6
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:** The requirement discusses enabling and disabling network capabilities.

5.6.1-D Preventing traffic from passing through EMSs

Requirement:	EMSs with multiple active network interfaces (including modems) SHALL NOT act as bridges or routers between networks that permit network traffic to pass through the electronic management systems.
Applies to:	Electronic device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Allowing network traffic to pass through a device that is not specifically designed to be part of the network/security infrastructure provides a possible method for malicious traffic to circumvent network security controls.
Source:	[NIST05] Security Control AC-6
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:** The requirement discusses enabling and disabling network capabilities.

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:*

5.6.2 Data transmission security

This section describes security requirements related to the encoding and decoding of data packets, and creating logical paths for transferring date between voting systems.

5.6.2-A Documenting network processes and applications

Requirement:	Access points such as covers and panels SHALL be secured by locks or tamper evidence or tamper resistance countermeasures SHALL be implemented so that system owners can monitor access to voting device components through these points.
Applies to:	Electronic device
Test Reference:	Part 3:4.1 “Initial Review of Documentation”
Discussion:	Understanding required network processes and applications is necessary for understanding the attack exposure of any given electronic device. This requirement generalizes [VVSG2005] I.7.5.2-b, which requires that manufacturers document all COTS hardware, and software communication devices used in the development and/or operation of the voting system if those devices are used on public communications networks. This requirement requires manufacturers to list network communication processes and applications required for the election system to function properly. There are no guidelines in the [VVSG2005] that require documentation of devices used for local networking. This requirement augments [VVSG2005] I.7.5.1-b-ii by mandating documentation of valid processes and applications associated with network ports and protocols.
Source:	[VVSG2005] I.7.5.1-b, I.7.5.2-b
Principle(s)/ Guideline(s):	*Security: Physical Security* Any unauthorized physical access to the voting system, ballot box, ballots, or other hardware, leaves physical evidence. Voting systems only expose physical ports and access points that are essential to voting operations, testing, or auditing. **Justification:** These guidelines align with this requirement.

5.6.2-B Prohibiting unnecessary communication between electronic devices

Requirement:	Electronic devices SHALL prohibit intercommunications between electronic devices except where required for normal function.
Applies to:	Electronic device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	In the interest of reducing the number of nodes accessing a given platform and potentially the voting data thereof, devices that have no need to interact over the network would be locally prohibited from those interactions. This reduces possible sources of network attack.
Source:	[NIST05] Security Control AC-6
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:** The requirement discusses management of network capabilities.

5.6.2-C Implementing integrity of data in transit

Requirement:	Electronic devices SHALL provide integrity protection for data in transit through generation of integrity data (digital signatures or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.
Applies to:	Electronic device
Test Reference:	Part 3:4.5 “Source Code Review”, 5.2 “Functional Testing”
Discussion:	Integrity protection ensures that any inadvertent or intentional alterations to data are detected by the recipient. Integrity protection for data in transit may be provided through the use of various protocols, such as IPsec VPNs and SSL/TLS. This requirement modifies [VVSG2005] I.7.5.1, which requires use of error correcting or detecting codes, by mandating use digital signatures or message authentication codes for data integrity. These provide addition protection against threats than error detecting codes, but do not offer data correcting capabilities. This requirement modifies [VVSG2005] I.7.5.1-a by specifying the use of cryptographic checksums (digital signatures and hashes) to be used to ensure information integrity in transit. This requirement modifies [VVSG2005] I.7.6.1, which requires the use of digital signatures in communications over a public network between a voter server and another device. This requirement extends [VVSG2005] I.7.6.1 by requiring integrity data for all data in transit. It furthermore includes a requirement to verify the integrity data for inbound data. This requirement extends [VVSG2005] 7.7.3-a, which requires protection against data manipulation on wireless communications, by requiring this protection on all data transmissions. Note that this document contains a prohibition against use of most wireless technology.
Source:	[VVSG2005] I.7.5.1-a, I.7.6.1, I.7.7.3
Principle(s)/ Guideline(s):	*Security: Data Protection* Voting systems prevent unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records. Voting systems protect the integrity, authenticity and confidentiality of sensitive data transmitted over all networks. **Justification:** This requirement aligns with these guidelines.

5.6.3 Application communication security

This section describes security requirements related to the communications of the voting application.

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-B Prohibiting unauthenticated communications

Requirement:	Electronic devices SHALL mutually authenticate using the devices’ unique system IDs before any additional network data packets are processed.
Applies to:	Electronic device
Test Reference:	Part 3:4.5 “Source Code Review”, 5.2 “Functional Testing”
Discussion:	Mutual authentication provides assurance that each electronic device is legitimate. Mutual authentication can be performed using various protocols, such as IPsec and SSL/TLS.
Source:	[NIST05] Security Control IA-3
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system authenticates administrators, users, devices and services before granting access to sensitive functions. **Justification:**

5.6.3-C Limiting network ports and shares and associated network services and protocols

Requirement:	Electronic devices SHALL have only the network ports and shares active and network services and protocols enabled as specified in Requirement 1.2.3- D.
Applies to:	Electronic device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Limiting network ports and shares and associated network services and protocols reduces the “attack surface” of the electronic devices. Attackers will have a diminishing chance of successful remote attack with each network port, share, service, and protocol that is disabled.
Source:	[NIST05] Security Control AC-6
Principle(s)/ Guideline(s):	*Security: Physical Security* Voting systems only expose physical ports and access points that are essential to voting operations, testing, or auditing. **Justification:**

	Security: Detection and Monitoring If the voting system contains networking capabilities, it employs appropriate modern defenses against network-based attacks. **Justification:**

5.6.3-D Documenting network ports and shares and associated network services and protocols

Requirement:	The manufacturer SHALL document all network ports, shares, services, and protocols required for the electronic device to function properly.
Applies to:	Electronic device
Test Reference:	Part 1:4.1 “Overview”
Discussion:	Understanding required network ports, shares (both visible and hidden/administrative), services, and protocols is necessary for understanding the attack exposure of any given electronic device. Based on local risk decisions, election officials will utilize the listing of required network ports, shares, services, and protocols to adjust configuration of an electronic device and the corresponding attack exposure.
Source:	[NIST05] Security Control AC-6
Principle(s)/ Guideline(s):	*Security: Physical Security* Voting systems only expose physical ports and access points that are essential to voting operations, testing, or auditing. **Justification:** *Security: Detection and Monitoring* If the voting system contains networking capabilities, it employs appropriate modern defenses against network-based attacks. **Justification:**

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:**

5.6.3-G Monitoring of host and network communication for attack and policy compliance

Requirement:	Electronic devices SHALL monitor inbound and outbound network communication for evidence of attack and security usage non-compliance.
Applies to:	Electronic device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Security usage non-compliance refers to instances where electronic device users are disobeying local policy. See NIST Special Publication 800-94 – Guide to Intrusion Detection and Prevention Systems [NIST07] for more information on host and network communication monitoring and attack prevention. This requirement extends [VVSG2005] I.7.5.1-b and I.7.5.2-a by requiring that intrusion detection systems monitor all inbound and outbound network connections, while [VVSG2005] 7.5.1-b and 7.5.2-a only require such systems monitor public communications network connections.
Source:	[NIST05] Security Control S-I-4, S-I-10, I.7.5.1-b, I.7.5.2-a
Principle(s)/ Guideline(s):	*Security: Detection and Monitoring* If the voting system contains networking capabilities, it employs appropriate modern defenses against network-based attacks.

5.6.3-H Prevention of host and network communication based attacks

Requirement:	Electronic devices SHALL provide the capability to stop inbound and outbound network attacks.
Applies to:	Electronic device
Test Reference:	Part 3:5.2 “Functional Testing”

Discussion:	See NIST Special Publication 800-94 – Guide to Intrusion Detection and Prevention Systems [NIST07] for more information on host and network communication monitoring and attack prevention. This requirement generalizes [VVSG2005] I.7.5.2-c, which describes the required capabilities of a voting device to stop an incoming attack over a network connection. This requirement further extends [VVSG2005] 7.5.2-c by requiring the ability to stop outgoing attacks as well.
Source:	[NIST05] Security Control S-I-4, S-I-10, I.7.5.2-c
Principle(s)/ Guideline(s):	*Security: Detection and Monitoring* If the voting system contains networking capabilities, it employs appropriate modern defenses against network-based attacks.