Draft Standard for Use of Wireless Communications Devices in Voting Systems

Draft Version March 2, 2005

2 March 2005

National Institute of Standards and Technology (NIST)

Provided for consideration by the technical Guidelines Development Committee (TGDC) and the Election Assistance Commission under the requirements of the Help America Vote Act (HAVA) of 2002

Written to address Resolution #35-05: Wireless

Acknowledgements

The National Institute of Standards and Technology (NIST) would like to acknowledge the individuals and groups who helped contribute to the preparation of this document. Members of the NIST voting team provided substantial assistance. Dr. Ronald L. Rivest, chair of the Security and Testing Subcommittee of the Technical Guidelines Development Committee (TGDC) provided strong leadership and guidance. NIST would also like to acknowledge the IEEE organization for permission to use excerpts from the IEEE P1583 Draft Standard for the Evaluation of Voting Equipment. A special acknowledgement goes to Tom Karygiannis, whose past work in evaluating security for selected wireless technologies provided a starting point and his review and input.

Authority

This document has been provided for consideration by the Technical Guidelines Development Committee (TGDC) and the Election Assistance Commission under the requirements of the Help America Vote Act (HAVA) of 2002.

Disclaimer

This document is a work in progress, provided solely as draft input to the TGDC. Portions of this document may change substantially. This document references some material from an unapproved draft of a proposed IEEE Standard, P1583. As such, the material is subject to change in the final standard. Because this material is from an unapproved draft, the IEEE recommends that it not be utilized for any conformance/compliance purposes. It is used at your own risk.

Table of Contents

Executive Summary

Based on Resolution #35-05 (Title: Wireless), NIST is directed to research and draft standards documents for the use of wireless communications devices in voting systems.

Since a blanket statement about wireless communications devices in voting systems is neither prudent nor appropriate given the wide variety of wireless communications devices and possible usage in the numerous and diverse voting systems, the approach to considering wireless communications devices in voting systems will be on a case by case basis.

To this end NIST will create a guide showing where wireless communications may potentially be placed in a particular voting system and some of the associated security risks. This guide will contrast the hype for wireless technology usage versus the real needs and/or requirements for wireless technology to improve the performance or operation of a voting system. The placements described are not to be construed as suggesting that wireless technologies should be used in these locations, nor is the list exhaustive of all current or future usage of wireless technologies placements. Nor does it replace those preexisting wireless requirements currently stated in the VSS2002 or IEEE P1583 /D5.3.1.

Just as a purely mechanical voting system can be modernized to use a purely computer automated voting system, so too can that system be modernized to include wireless technologies. Therefore, it is not a question of will wireless technologies be used, but rather a matter of time until wireless technologies are used. The answer to this question has already been answered because wireless capabilities are present in some voting systems today. A better question to ask is, Should it be used and, if so, under what circumstances? Again the answer to this question is very clear. Any wireless technologies should be used when it improves the performance or operation of the voting system without introducing any other problems or issues (e.g., security). Thus if requirements are written which can only be satisfied by wireless communicating devices, then they should be used. Otherwise they should not be used just because they can be.

An exhaustive investigation of all possible wireless technologies, or more importantly all implementations of wireless technologies will never be practical. Therefore specific wireless technologies will only be used as examples.

1. Introduction

In general wireless communications devices introduce new functions and features, as well as new issues and concerns, especially security. Since the term, wireless communications, is such a broad term, it is important that agreement is reached on the term, its meaning, and its application, before any recommendations are made regarding its use in voting systems. In order to reach a common understanding for the term, wireless communications, an entire section is devoted to the subject. Since there is a wide variety of wireless communications devices in use in the world outside of the voting system environment, some envision how these may be included into a voting system. Others have already implemented wireless communications into their voting systems [reference]. If these voting systems use commercial off the shelf (COTS) wireless communications devices, then they have similar issues and concerns as do any COTS product for use in voting systems.

This document explores the meaning of the term, wireless communications, in order to lay the ground work for considering wireless communications devices in voting systems. The description covers in general terms the issues and concerns with any wireless communication system transferring data. The document next explores places where wireless communications might be used or already is being used in a voting system. [Note: When wireless communications are being used in an existing voting system, then that system is identified for information only, and is not to be construed as a de-facto -standard, -use or -implementation for a voting system, nor is it to be considered an endorsement or a promotion for that device, manufacturer, or user.] The placements of wireless communications within a voting system follows the structure and layout of the Voting system standard (VSS) 2002. Wireless communications in a voting system is reconsidered from another perspective in a separate section. Finally recommendations are made on wireless communications in voting systems.

The next section (2) gives an introduction of wireless communications devices and some of the items requiring further examination. The section (3), “A voting system,” will cover possible wireless communications devices placement following the structure and layout of the VSS2002. Section (4), “physical locations,” provides another perspective of wireless communications in voting systems. The last section (5) contains comments and recommendations.

2. Wireless communications

A discussion of wireless communications, its allure, and its risks is necessary before going any further. The following subsections describe these. The first section opens with a simple definition and two easy to understand examples that are used to explain the terms and components of wireless communications. These two examples are then used in the other subsections to demonstrate the risks associated with wireless communications. With this background a common understanding will be assumed in order to proceed to deal with the concerns and issues with the possibility of using wireless communications in voting systems.

2.1. Simple definition

A simple definition of wireless is “any means of communication that occurs without wires.” [TK5105.59.P68-2003] This is an extremely broad definition, but it is a start. For a communication to occur there must be one sending device (i.e., a transmitter) and at least one receiving device (i.e., receiver). If there are no wires, then what is used to transfer the signal from the transmitter to the receiver? The obvious answer is the air. For example if one speaks and another listens, is this wireless? Yes, it is. The signal (i.e., sound) uses vibrations to move the molecules in the air so that the sound waves are received by the inner ear (note that both the one speaking and the one listening hear). Is sign language wireless? Again the answer is yes. In this case it is the light passing through the air that permits the eye (i.e., receiver) to see the hand signals. For both of these examples the wireless communications is not one sided (i.e, unidirectional). Both persons are able to send, as well as receive. The term that is given to devices that can both send and receive is called a transceiver.

2.1.1. Wireless characteristics

Here the simple definition and examples are expanded upon to further explain the characteristics of wireless communications. Wireless communications provide connectivity between at least two devices (a transmitter and a receiver) by using energy in various forms through the air instead of using wires or cables. Sometimes the energy is in the form of lightwaves (e.g., infrared, visible light, or ultra violet) and sometimes the energy is in the form of radio frequencies.

2.1.1.1. Transmission path:

The path by which the energy travels (i.e., radiates) may be narrow, wide, or omni-directional. The ability of the energy to pass through objects in its path or be reflected by them, is dependant upon the characteristics of the energy used in the transmission.

Some transmission paths may require line of sight (LoS), like microwave and infrared, while others may not.

Using the sign language example we see what is meant by line of sight (LoS). The ability to understand the sign language depends upon whether or not one can see the hand presenting the signals. One’s sight may be blocked by the person doing the sign language, if he is standing behind the signer. One’s sight may be blocked by facing in a direction that is not towards the hand that is signing. One’s sight may be block by another object (e.g., another person, a wall, a plant, or a door). Of course, there is the case that the distance between the person giving the hand signals and the person trying to see the hand signals is too far away to be seen unaided. This distance in wireless terms is called the range.

Using the speaking example we see what is meant by broadcasting or omni-directional. The sound waves move away from the speaker in all directions. The sound waves go around some objects and through others. The sound waves get weaker as they get farther away from the source (transmitter) or pass through objects. At some distances the sounds waves are just too weak to be heard without assistance. The area where the sound is strong enough to be received in wireless terms is called the coverage area.

Experimental data that show the effects of construction material (e.g., concrete walls and glass) on attenuation (i.e., the ability for certain frequencies to pass through, to be decreased, or to be stopped) of electromagnetic signals are given in NIST Construction Automation Program Report No. 3: Electromagnetic Signal Attenuation in Construction Materials. From this report it should be easy to see that defining the coverage area or range of a wireless signal is strongly dependent on the surrounding environmental characteristics and something that cannot be controlled.

2.1.1.2. Type of wireless communicating devices:

The wireless communicating devices implement protocols that are design in one of two types: peer-to-peer and master-slave. Peer-to-peer devices implement the same functions and features so that any device may communicate freely with any other device. Master-slave devices implement functions that are different for master and slave. The master device has more functions and controls the slave devices. The slaves devices have less functionality and must communicate only with the master device.

A thorough examination of the protocols used within each wireless communications device will need to occur before a recommendation on that particular wireless technology's use is provided. [Note that this applies to testing criteria or what to look for. A technology by technology application and security analysis is not a maintainable approach for all current or future proofing of wireless communications devices for voting systems].

2.1.1.3. Categories of wireless:

There are numerous ways to categorize wireless communications. Here are just a few. Wireless communications may be categorized by their intended range such as body area network (BAN) less than 1 meter, personal area network (PAN) less than 10 meters, local area network (LAN) less than 100 meters, metropolitan area network (MAN), or wide area network (WAN). Wireless communications may be grouped by the frequency(ies) used (i.e., band designations). (See Table 2) Wireless communications can be considered private or public, regulated or unregulated, or licensed or unlicensed.

The Radio Frequencies (RF) used by wireless communications devices are governed in the United States of America by the Federal Communications Commission (FCC). The tables below show the entire frequency spectrum, of which radio frequencies are just a part. The Table 1 presents the technical characteristics, while Table 2 presents the band designations and which of those are considered under the category of radio frequency.

	minimum	maximum	units
Frequency	0 Hz	10^{25} Hz	Hz (Hertz)
Radio Frequency	3 kHz	300 GHz	
Wavelength	0 A	3x10^{-7} A	A (Angstrom)
	0	3x10^{-17}	m (meter)
Usage	Government exclusive	Non government exclusive	Shared

Table 1 – Frequency Spectrum

Band designations	Frequency ranges	Radio frequency
Very Low Frequency (VLF)		Upper part
Low Frequency (LF)		All
Medium Frequency (MF)		All
High Frequency (HF)		All
Very High Frequency (VHF)		All
Ultra High Frequency (UHF)		All
Super High Frequency (SHF)		All
Extremely High Frequency (EHF)		All
Infrared		None
Visible light		None
Ultra violet		None
X-Ray		None
Gamma Ray		None
Cosmic Ray		None

Table 2 - Frequency Spectrum (Band Designations)

Some wireless technologies have been designed to replace wires. In a current voting system, where are the wires that may be replaced by wireless technologies? Some examples are the wires and cables that provide connectivity now serving as local area networks (LANs), wide area networks (WANs), and input (e.g., keyboard or mouse) or output devices (e.g., printer or earphones) connections. These will be examined more closely in their respective sections.

2.2. The Allure

Everything wireless appears to be the current trend, however, the necessity is not. “Gets rid of the wires,” “Look mom, no wires,” and “I’m mobile” are just some of the hype reasons for promoting wireless communications. Having no wires is a convenience, but is it really a necessity? In some cases (e.g., a ship out at sea, an airplane in flight, or a satellite in space) the answer may be yes, but in many cases it is not (e.g., voting system). If a device needs power by means of alternating current (AC) power outlet, then having wireless does not remove all of the wires. This defeats the wireless feature which permits mobility as a necessary requirement. Portability, which just permits a device not to be fixed to a single place, but fixed to a place for a prolonged period of time, may be an advantage, provided it is still within the wireless coverage area and provides AC power. Pervasive computing, sensor networks, and mesh networks are just a few of the hot subject terms that promote and hype wireless communications.

2.3. The Risks

Wireless communications do not come without risks, but what are they and how can they be avoided or at least reduced are questions with answers that are open for debate. Sometimes the risks are unknown, or at least strongly debated. For example, the cellular systems have been debating the issue of whether or not cellular handsets and their energy emissions cause damage to the brain. Microwave communications are nasty. Many of us have microwave ovens and by looking at the results, one would not want to be within the path of microwaves used for wireless communications. So it is with these specific wireless examples, however there are general known risks associated with any wireless communication.

2.3.1. Inherit wireless risks

Wireless communications have at least two major concerns (broadcast media and interference). Both may be viewed as a physical or security issue.

2.3.1.1. Broadcast media:

The very nature of wireless communications poses issues and concerns for functionality, performance, reliability, and security. Wireless communications broadcast energy (i.e., signals). This broadcasted energy can be received by any compatible receiver in range (LoS) or coverage area. By the same token any other device can transmit to another compatible device. A visual determination of the devices communication using wireless technology is not readily available, unlike the physical cable connections used for communications.

Thus preventing a signal from being received by an unwanted receiver can only be prevented by securing the signal distance (range or coverage area). Securing the signal distance is an expensive proposition and for most part impractical for anything larger than a room. (Note: The National Security Administration (NSA) attempts this on the scales of buildings.)

The broadcast (physical) nature of the media is not to be confused with the term, broadcast (logical), as used by the higher layer protocols when broadcasting frames, packets, or messages to multiple devices. This type of broadcast (logical) is accomplished by one of two logical methods. One method is by using an address (identifier) that specially marks a frame, packet, or message to be received by any compatible receiving device. Another method replicates the same frame, packet, or message for each device that is intended to receive the frame, packet, or message.

Using either method leaves open the ability for an unintentional receiver to receive the frame, packet, or message. It is obvious in the first, since all that is required to receive is a compatible receiver. In the second, one only needs to add the unintentional address to the list of devices to replicate the frame, packet, or message in order to receive or override the address filtering to accept all information with any address.

Other security methods (e.g., encryption) are required to reduce the risk of an unintentional device receiving the frame, packet, or message and being able to understand its contents once it is received.

2.3.1.2. Interference:

Some wireless technologies are susceptible to other electromagnetic interference. This interference may be controllable or it may not. That is, one may have the ability to control the presence of wireless communications devices that emit electromagnetic interference or one may not. Personal wireless technology usage (i.e., walk-in / walk-by) may not be preventable and may cause interference to voting systems, if they use common frequencies. Even though some airlines, movie theaters, and conferences ask that cell phones not be used, they are. Therefore, a voting system must guarantee that if it uses wireless technology that it cannot be affected by walk-in personal wireless devices (i..e, unintentional interference). However, an intentional interferer could be used to create enough interference as to disrupt the wireless communications and create a denial of service (DoS) attack.

LoS wireless technologies can easily be disrupted by placing an object (e.g., a finger) over the portal. Incandescent or florescent lights have been known to cause interference for infrared systems, thus warning labels on remote controls for video cassette recorders (VCRs), digital video disk (DVD) players, and televisions (TVs).

Thus interference must be examined as part of the evaluation to use or not to use wireless communications devices in a voting system.

2.3.2. Specific wireless risks

In the simplistic examples given above, one can now begin to understand the risks involved using wireless communications. The following risks are easier to do with wireless communications than with wired communications.

2.3.2.1. Eavesdropping:

If a conversation is occurring between two people, it is very easy for another person to listen in on the conversation. This is the advantage of broadcasting (i.e., one transmitter and multiple receivers). However it is just this feature that makes wireless communication insecure. How do you ensure that only those who you want to listen in on the conversation do so and all others cannot? Unlike communications over a wire or cable that requires a physical tap to eavesdrop (i.e., intercept the signal), wireless communications eavesdropping is particularly simple. Just listen.

Countermeasure:

If the conversation is occurring in a language that you do not understand it may be useless to you. If that same conversation was recorded, you could find someone who would be able to understand it. This speaking another, or foreign, language is like using encryption when it comes to electronic communications.

2.3.2.2. Interference:

If a conversation is in a room filled with many people talking or signing, it becomes difficult to hear or see and understand just one conversation. The coverage area for the conversation shrinks as does the range for signing. The same is true for electronic devices when wireless communication is used.

Countermeasure:

Interference between wireless communication systems can be reduced by using different frequencies, isolating coverage areas, and managing power emissions. The solution of using different frequencies eventually fails because frequencies are a limited resource and there are more systems wanting to use said resources. Isolating the coverage areas by means of shielding it from unwanted energy and preventing its own leakage is an expensive solution. The ability to increase the amount of energy during transmission also eventually does not work, because if every device does it, the relative increase would be zero.

2.3.2.3. Jamming:

If one person starts speaking very loudly just to be annoying, it is possible for a conversation to be completely interrupted. Jamming is the intentional extreme form of interference. In this case the amount of interference is so great that the wireless communication is interrupted completely. From a security perspective, this is what is known as a denial of service attack.

Countermeasure:

Since jamming is a form of interference, the methods for reducing the risk are the same.

2.3.2.4. Masquerade:

If a conversation is occurring and another person is able to imitate the voice of the speaker, one might be able to pretend to be the real speaker. In this case the person listening would need to not be able to confirm (i.e., by sight) the real speaker. For wireless communication a device can to pretend to be the intended receiver or transmitter, or both (i.e., man in the middle).

Countermeasure:

Authentication.

2.3.2.5. Modification:

Modifying a live in person conversation is hard to envision, but since some English words sound alike, it is possible for someone to inject a similar sounding word so that the listener does not hear the original word. Since there is no physical path (i.e., cable of wire between communicating devices) to secure, it is relatively simple to inject signals into the wireless communication’s path.

Countermeasure:

Encryption is used to hinder the ability to modify data.

2.3.3. Security issues

The specific security related issues (i.e., Authentication, Confidentiality, Data integrity, Non repudiation) are addressed under the appropriate areas for the voting system in the following sections.

A secure system today is a compromised system tomorrow. Such is the state of technology and security. One must keep this in mind. There is no absolute future protection for all security risks. It is just the best information available at that particular point in time.

3. A voting system

A voting system is defined in VSS Volume I – section 1.5.1
"*A voting system is a combination of mechanical, electromechanical, or electronic equipment. It includes the software required to program, control, and support the equipment that is used to define ballots; to cast and count votes; to report and/or display election results; and to maintain and produce all audit trail information. A voting system may also include the transmission of results over telecommunication networks.*

Additionally, a voting system includes the associated documentation used to operate the system, maintain the system, identify system components and their versions, test the system during its development and maintenance, maintain records of system errors and defects, and determine specific changes made after system qualification. By definition, this includes all documentation required in Section 9.4.

Traditionally, a voting system has been defined by the mechanism the system uses to cast votes and further categorized by the location where the system tabulates ballots. However, the Standards recognize that as the industry develops unique solutions to various challenges and as voting systems become more responsive to the needs of election officials and voters, the rigid dichotomies between voting system types may be blurred. Innovations that use a fluid understanding of system types can greatly improve the voting system industry, but only if controls are in place to monitor and control integrity through the proper evaluation of the system brought for qualification.

As such, vendors that submit a system that integrates components from more than one traditional system type or a system that includes components not addressed in this Standard shall submit the results of all beta tests of the new system. Vendors also shall submit a proposed test plan to the appropriate independent test authority recognized by the National Association of State Election Directors (NASED) to conduct national qualification testing of voting systems. The Standards permit vendors to produce or utilize interoperable components of a voting system that are tested within the full voting system configuration."

From this definition five voting systems are explicitly stated in VSS 2002 Volume I, sections 1.5.2 through 1.5.6. These five voting systems are listed here and show where wireless communications may be introduced (intentionally or unintentionally) into a voting system.

- **Paper-based voting system**
  If an electronic input device is used, this device may be connected via means of a cable or wirelessly. Having the electronic input device wired would lend itself better for not misplacing the device, as if a wireless input device were used. This is similar to a writing instrument (e.g., a pen) at a bank teller window. They are not attached for security reasons (i.e., loss of a high priced pen) or at add to functionality of the writing instrument, but rather for convenience (i.e., to have a pen present and prevent its accidental removal).
- **Direct record electronic (DRE) voting system**
  If this DRE voting system provides *"a means for transmitting individual ballots or vote totals to a central location for consolidating and reporting results from precincts at the central location,"* then the means may be by using wireless technologies.
- **Public network direct record electronic (DRE) voting system**
  "*However, because transmitting vote data over public networks relies on equipment beyond the control of the election authority, the system is subject to additional threats to system integrity and availability.*" It is possible that there is a wireless link/segment within the public networks, thus hidden wireless communicating devices (e.g., microwave or satellite link) concerns must be considered, which are outside the control of the election authority.
- **Precinct count voting system**
  Printing out the results may be through a built-in printer or an adjunct printer. If it is an adjunct printer the means by which the data from the recorder is passed to the printer may be by means of a wireless connection. Transmitting the results to a central location over the public telecommunications networks are the same issues as for the public network DRE.
- **Central Count voting system**
  "*The systems produce a printed report of the vote count, and may produce a report stored on electronic media.*" The device used to print the report may be using wireless communications between it and the central count voting system. If a report is produced on electronic media, this may be through wireless communications (i.e., wireless external hard disk or memory stick).

3.1. Wireless possibilities as per the current VSS 2002

More detailed wireless devices and detail usage will be described in the following sections, which follows the structure and layout of the VSS 2002 Volume I, sections 2 through 9. Each section is examined for the possibility of wireless communications being applied, where it currently exists, and suggests additional considerations.

VSS 2002 Volume 1, Section 2 - Functional Capabilities

- 2.2 Overall capabilities

2.2.1 Security –

“a) Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability.”

If wireless communications are to be secured, then they need to be at least identifiable. Identifiable means that a visual (or audible) indication is present when wireless communications are in operation. However since most wireless communications operate in a broadcast manner, it is possible that there is more than one communication path established at one point in time. If so, then the visual indication is not sufficient to detect intrusion, if it occurs during a period when an intentional communication is occurring, which is the best time to attempt a break-in. Other security mechanisms are required to prevent multiple accesses through the same wireless communication method.

“b) Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.”

For wireless systems the intended conditions are hard to maintain or foresee and ensuring that the wireless communication is used in only the intended manner requires limiting its wireless characteristics, which may not even be possible for some wireless communications.

“c) Use the system’s control logic to prevent a system function from executing if any preconditions to the function have not been met.”

This is entirely dependent on the hardware implementation, if wireless communications are used.

“d) Provide safeguards to protect against tampering during system repair, or interventions in systems in system operations, in response to system failure.”

For wireless systems this can introduce more problems. For example wireless is yet another piece that may be compromised. Replacing a wireless device may lead to other failures or other configuration problems (e.g., if MAC address filtering was used)

“e) Provide security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation, testing, and operation.”

This would need to be done on a case by case basis, since the administrative tasks are different. Having wireless systems introduced would only add to the level of complication and number of procedures needing to be completed.

“f) If access to a system function is to be restricted or controlled, the system shall incorporate a means of implementing this capability.”

The means for restricting or controlling wireless systems will be at best an off switch because once wireless communications are on it is difficult to restrict or control.

“g) Provide documentation of mandatory administrative procedures for effective system security.”

For wireless communications systems there are general practices, but eventually it requires a meticulous risk assessment of the particular wireless communication technology in use.

2.2.2 Accuracy –

If wireless communications are used, some of them may increase the amount of electromagnetic stresses the voting system must withstand. Also the wireless communications must withstand a level of electromagnetic stress. However this level is entirely dependent upon the type of wireless communications.

2.2.3 Error recovery –

For wireless communications this is both a help and a hindrance. If wireless communications were being used before the non-catastrophic failure, it is almost impossible for some wireless communications to return to the exact state. However wireless communications might be an alternative method for recovering from another communications error (e.g., land line phone line) in order to keep a system operational.

2.2.4 Integrity –

Wireless communications may satisfy protection against the interruption of electronic power, if batteries are used instead of mains, but the use of some wireless communications may void the protection of a system against generated or induced electromagnetic radiation.

2.2.5 System Audit –

If wireless communications were used additional information of this activity (i.e., events) will need to be recorded as part of the audit for the system.

2.2.6 Election Management System –

The data produced by this system and the data required by this system must be entered or retrieved. The means to accomplish this could be through wireless communications.

2.2.7 Accessibility –

2.2.7.2 b) Providing audio information and stimulus for item 6) alone, the headphones could use wireless technology. However with the inclusion of item 7) wireless would be prohibited in this specific part of a voting system. Item 8) may allow for a remote device for volume control, which could use wireless communications.

2.2.7.2 c) requires provisions for a special type of wireless communications, if telephone style handsets are used to provide audio information.

2.2.7.2 d) contains a requirement that some wireless communications must meet in order to avoid electromagnetic interference with hearing devices. This brings forward another very important requirement that no wireless communications should interfere with any medical device (e.g., pace makers).

2.2.7.2 e) the ability to adjust electronic image displays: This may be through a remote device, which uses wireless communications.

2.2.7.2 f) provide an input method: This input method may be through a wireless method.

***2.2.10 Telecommunications* –** All of these items are minimally required, if wireless communications are used instead of or in cooperation with public networks.

Voter Authentication
Ballot Definition
Vote Transmission to Central Site
Vote Count
- polling place
- precinct
- central count

List of Voters

- ***2.3 Pre-voting capabilities***

- ballot preparation
The method of creating the ballot may be done through wireless means (i.e., mouse and keyboard), however since the assumed entry method is immediate recognition, the security risk is low, except for protection of any password typed to enter a system.

- election programming
The method of creating the ballot may be done through wireless means (i.e., mouse and keyboard), however since the assumed entry method is immediate recognition, the security risk is low, except for protection of any password typed to enter a system.

- ballot and program installation and control
The means to transfer (install) the ballot and program from one device to another may be by means of wireless communications. Further investigation required.

- readiness testing
If wireless communications devices are used in this area, then testing becomes a lot more complicated. Further investigation required.

- verification at the polling place
If wireless communications devices are used in a voting system, then they become another item needing to be verified for correct operations. The conditions (e.g., interference) during the verification may not be the same as when used.

- verification at the central counting place
If wireless communications devices are used in a voting system, then they become another item needing to be verified for correct operations. The conditions (e.g., interference) during the verification may not be the same as when used.

- ***2.4 Voting Capabilities***

2.4.1.3 DRE System Standards – a) complicates this since a seal will not prevent access to wireless communicating devices. Physical security seals are only useful when there is something that physically needs to be kept from moving, however there is not necessarily any moving part, if wireless communications is available. A password helps to prevent access to the system, but a separate password may be necessary to prevent access through the wireless portal. “data code recognition”.
The means by which election officials can active, allow, disable, enable, or prevent a voter to cast a vote may be by wireless communicating devices. If so, then wireless requirements need to be specified.
2.4.3.1 Casting a ballot – items b), e), and f) are of interest if wireless is used.
2.4.3.3 – a)”… linking to other information sources” must be prohibited – Hard to secure, if wireless is in use.

- 2.5 Post-voting capabilities

2.5.1 Precinct count - items a) and e) for wireless consideration (i.e., must prevent casting votes after polling place has closed and preclude reopening of the polls once closed.

2.5.3.1 g) if transmission over telecommunications lines uses wireless communications or is replaced by wireless communications, then this becomes a real issue.

2.5.3.2 - a) if a wireless communication is operational during this phase, then its use as an access must be prevented.

2.5.3.2 - d) if transmission over telecommunications lines uses wireless communications or is replaced by wireless communications, then this becomes a real issue.

2.5.4 - b) *"Provide no access path from unofficial election reports or files to the storage devices for official data:"* If the same wireless communication is used to retrieve the unofficial and official report from the systems being kept separated, then there is no way to provide "no access path" for once the wireless is on any device can send or receive the wireless signal, unless other procedural security measure are taken.

- ***2.6 Maintenance, transportation and storage capabilities***

VSS 202 Volume I, Section 3 - Hardware Standards

3.2.2 Environmental Requirements – Electromagnetic signal environment, including exposure to and generation of radio frequency energy. This is applicable to some wireless communications, but not to others (i.e., infrared).

3.2.2.9 Electromagnetic Radiation
3.2.2.10 Electromagnetic Susceptibility

This is applicable, but the requirements need to be updated to expand the frequency range, since some of the most currently used wireless communications used frequencies greater than 1000 MHz.

3.2.2.11 Conducted RF Immunity
3.2.2.12 Magnetic Fields Immunity
3.2.2.15 data network requirements

3.2.4.3.1 Activity indicator – There needs to be a separate indicator for wireless communications, if present and/or operational.

VSS 2002 Volume I, Section 4 - Software Standards

Nothing obvious

VSS 2002 Volume I, Section 5 – Telecommunications Standards

5.1.1 Types of Components –

Lists three types of wireless (wireless, microwave, and VSAT) for dial-up and wireless connections (RF and infrared). Therefore all items under telecommunications section 5 also apply to wireless communications.

5.2.6 Integrity - c) single point of failure: Wireless communications may be used as an alternative (i.e., backup).

VSS 2002 Volume I, Section 6 – Security Standards

6.3.1 b) "Control physical access to a telecommunications link if such a link is used." When wireless communications is used as part of the telecommunications link, there is no physical access that can be controlled.

6.4.1 c) This requirement is tricky at best to try and guarantee when wireless communications are used.

6.5 Telecommunications and Data Transmission

6.5.1 Access Control –

Same as for telecommunications 6.3.1 b) which is not possible if wireless communications are used.

6.5.2 Data integrity –

If verification occurs at the voting system application level, then it already covers wireless, since most wireless technologies just replace the low levels (e.g. physical, data link, and/or network layers)

6.5.3 Data interception Prevention –

The prevention methods apply to wireless communications, but there is no way to detect that data was intercepted. (An inherit problem with wireless).

6.5.4 Protection Against External threats –

All applies to wireless communications as well.

6.6 Entire section applies and needs to be expanded for specific wireless communications considerations. Appendix B rewrites this clause for private wireless communications.

VSS 2002 Volume I, Section 7- Quality Assurance

Nothing obvious

VSS 2002 Volume I, Section 8 – Configuration Management

Nothing obvious

VSS 2002 Volume I, Section 9 – Overview of qualifications Test(ing)

9.5.1.1 Hardware exemption for COTS – No commercially available wireless hardware has demonstrated that its performance would satisfy security requirements.

9.6.2.4 If wireless communications devices are used, then this would need to be included here. This is the place to examine electromagnetic interference both generated and received by the voting system. However the sample set is too small.

4. Physical locations

This section will examine in more detail the places and times where wireless communications may be used and the security issues associated there and then. This section provides a different view of the voting system as listed in section 3. Two perspectives need to be addressed: the place and the time. The place will be organized according to the type of voting system and the time will be organized according to the functional capabilities. Figure 1 shows the possible wireless communications and the information transferred.

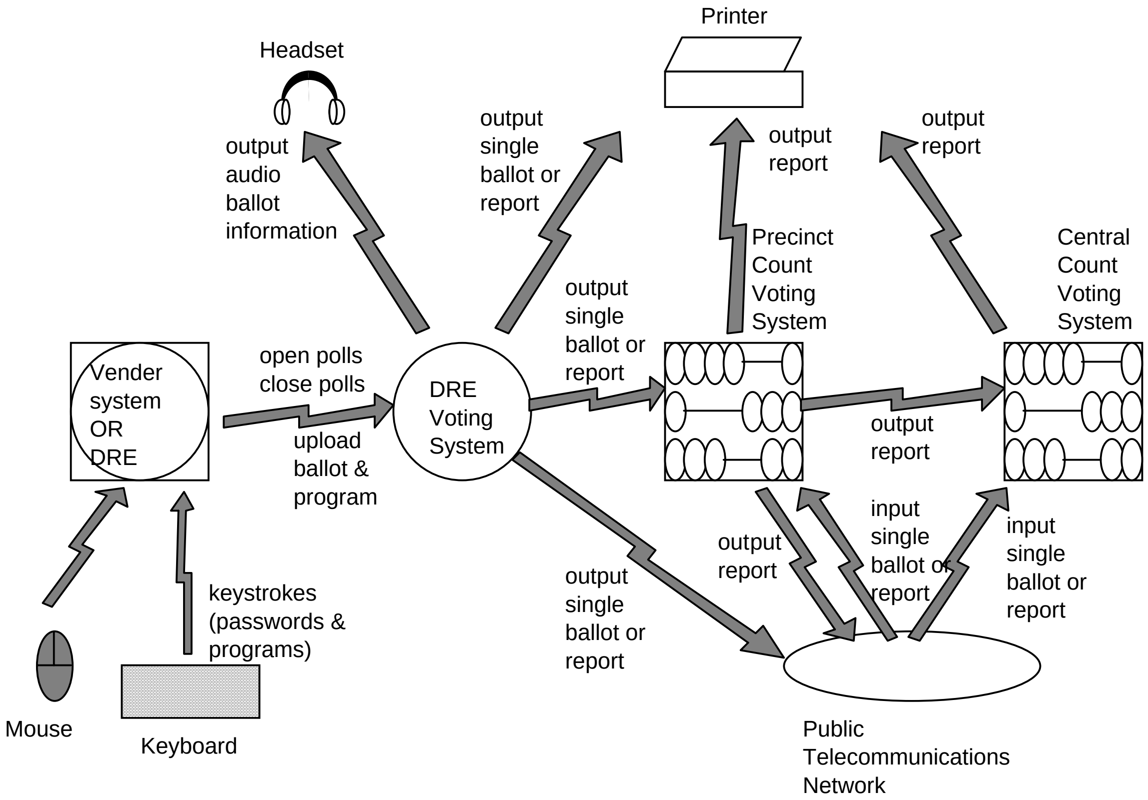
Printer
Headset
output audio ballot information
output single ballot or report
output report
output report
Precinct Count Voting System
Central Count Voting System
output single ballot or report
Vender system OR DRE
open polls close polls
DRE Voting System
upload ballot & program
output report
input single ballot or report
input single ballot or report
output report
output single ballot or report
keystrokes (passwords & programs)
Mouse
Keyboard
Public Telecommunications Network

Figure 1 – Wireless placement and information flows.

4.1. Place

The placement of wireless communications into a voting system is highly dependent on the type of voting system used, when it is used and how it is used.

4.1.1. Paper-Based Voting System

The paper ballot itself has no wireless possibilities, however its creation, usage, and tabulation systems may. The output device used to create the paper ballot may be connected by wireless means. The use of wireless in this case is deemed to be a low security risk, since it is easily verified that the paper ballot is correct. The use of a wireless communications device as an electronic input device, for the paper-based system with the current restrictions that prohibit the device to independently record, store, or tabulate the voter's selections, it is hard to foreseen just what the electronic input device would be communicating with and what information would be needing to be transferred. Extracting the tabulated votes from a paper-based system may be through wireless communications. The items needing to be protected are the counts and access to the wireless communicating systems. One would need to protect the counts from interception and modification. Protecting the access to the wireless communicating systems is to prevent the system from being compromised, which could mean making the system inoperable, destroying the existing data (counts), or modifying the system.

Making the system inoperable is not detrimental, since a paper version exists, which may be hand counted. The same is true for the counts. However modification of the system may not be as readily identifiable or may not be identified unless the vote count by the machine is audited against the paper ballots. In any case the data transferred over the wireless communications must be encrypted to prevent eavesdropping.

4.1.2. Direct Record Electronic (DRE) Voting System

Wireless communications capability in DRE voting systems can be classified as input, output, or distribution of data. A DRE voting system must be programmed. If the program is to be loaded on the DRE using wireless means, then the program and access to the systems must be protected. The ballot information may also be what is distributed wirelessly.

A wireless coupling for assistive devices, as currently defined, cannot be secured. However since its coverage area is small and it is only an output device, the risk is considered low.

4.1.3. Public Network Direct Record Electronic (DRE) Voting System

If a DRE voting system is using the public network, it is important to know what and when any wireless within that public network is being used.

4.1.4. Precinct Count Voting System

If the precinct count voting system is using wireless communications to receive individual cast ballots or transmitting the vote count results, then this information must be protected from eavesdropping and modification.

4.1.5. Central Count Voting System

If the central count voting system is using wireless communications to receive the vote count results, then this information must be protected from eavesdropping and modification.

4.2. Time

The time when wireless communications are being used is important in determining the security issues.

4.2.1. Overall capabilities

All of the listed items apply to wireless communications.

4.2.2. Pre-voting capabilities

Pre-voting capabilities consist of ballot preparation, election programming, ballot and program installation and control, readiness testing, verification at the polling place, and verification at the central counting place.

Whether of not wireless communications devices (e.g., mouse or keyboard) are used to prepare the ballot or program the election, the immediate visual response to the action is known. However if one intercepts the entire ballot preparation information, it will be easier to knowingly corrupt it. If the wireless uses a line of sight technology (e.g., infrared), the likelihood for interception is small. If the wireless uses a non-line of sight technology (radio frequency), the likelihood goes up, thus justifying the need to at least encrypt the wireless communications. The possibility that multiple similar input devices (i.e., two mice or two keyboards) could be used should be prohibited.

Assuming that one would not prepare the same ballot or election on each device, a method of distributing the same ballot or election may occur using wireless communications. In this case of ballot and program installation and control, the data is critical to the proper operations of the voting system. The use of wireless, though convenient, is discouraged. Procedures should be in place to verify the ballot and program once installed in any case, but especially if wireless means was used. The voting system itself should be verified that no other modification has occurred while the wireless communication was active. All of this is assumed under the readiness testing, verification at the polling place, and verification at the central location.

4.2.3. Voting capabilities

Voting capabilities are opening the polls, casting a ballot, and for all DREs activating the ballot, augmenting the election counter, and augmenting the life-cycle counter.

If procedures are in place to visually verify that a DRE is open and ready for use after receiving any signal to open the polls via a wireless signal, then the risk of using wireless in this case is minimal. The risk that still must be protected is the access to the DRE over the wireless communications.

If the DRE uses wireless communications to transmit ballot information from it to another device (e.g., printer or precinct count voting system) after every ballot is cast, then the wireless communications shall not be used if that DRE is used to service the curb voting. This is a requirement since there is no way to secure the wireless less link at the curb side (i.e., open air) to ensure voter privacy.

If the DRE uses wireless communications to transmit ballot information, a continuous stream of data should be sent, so that an eavesdropper does not know when the data being sent is the ballot or just vacuous data, which is to prevent isolation of a single transmitted ballot. However since many wireless communications use a medium access control that is carrier sensed multiple access (CSMA), the performance of the wireless communications would be significantly degraded due to the extra vacuous data being transmitted.

If wireless is used during the elections, it will be susceptible to interference from voter carried items (e.g., cell phones, wireless PDA), therefore the DRE shall be able to operate without wireless communications, for at least the duration of a voter to a cast ballot, but should also include the time the voter nears the polling place until the voter leaves the polling place.

4.2.4. Post-voting capabilities

Post-voting capabilities include closing the polling place (precinct count), consolidating vote data, producing reports, and broadcasting results.

If procedures are in place to visually verify that a DRE is closed and no more votes can be cast after receiving any signal to close the polls via a wireless signal, then the risk of using wireless in this case is minimal. Prevention of premature closing of the polls must be protected, if wireless communications are used. The risk that still must be protected is the access to the DRE over the wireless communications.

The use of wireless communications to transmit consolidated vote data or report, would have minimal risk, if procedures are in place that compare the results sent over the wireless communications and the results that are stored in the DRE before making an official result.

Use of wireless communications during the broadcasting of unofficial results shall not be via the same wireless communications as was used by the DRE, since the wireless communications access path cannot be prevented. Otherwise this would violate the requirement that no access path from unofficial electronic reports or files to the storage devices for official data.

4.2.5. Maintenance, Transportation and Storage capabilities

While any wireless capable voting system is being stored or transported, the wireless capability must be disabled (i.e., non-functioning). This is to prevent access to the physically secured and stored device be means of the wireless link, which cannot be physically secured.

The only possible exception for a wireless system to be active during storage or transportation is if a radio frequency identification (RFID) is being used. RFID may be used if one wants to track the physical location of the voting devices, one may employ radio frequency identification. RFID is a wireless technology that would be used for asset tagging, identification, and tracking. This would be similar to the physical security seal identification tags currently used. In this case the RFID shall not be coupled, interfaced, or integrated into the voting system’s program or operating system. It must be stand alone and self contained. If RFID is used, it shall not interfere in any way with the wireless used for the voting system.

Maintenance of a voting system shall not be through the wireless capability, unless the wireless capability is having the maintenance performed on it.

4.3. Wireless usage

The dangers of wireless usage for a voting system can be categorized into two groups: the information transferred and the access to the devices exchanging the information. The information is usually either being distributed or collected. Distributed information (e.g., ballot definitions, open or close polls signal) is sent to all systems. Collected information (e.g., individual votes, reports) is retrieved from systems. Access to the wireless communicating systems is a major concern because of the damage that can be caused by a compromised system. In this case security measures must be in place to prevent unauthorized access. This means limiting services available using wireless communications, authenticating the user and the device itself, and installing firewalls.

Wireless practical solutions/problems:

- If a wireless device operates using batteries, then the device must be designed to operate for the duration of the voting period without needing replacement.
- If a wireless device operates using batteries, then the type of battery used needs to be readily available and storage of the batteries for long term. Many battery powered devices already state that the batteries should be removed from the device, if the device will be stored for a long period of time.

5. Recommendations

After reviewing the current requirements of the VSS 2002, there is no technical requirement or necessity to include or use any wireless communications in a voting system, even though possibilities to use wireless communications exist. Currently some wireless is listed under the VSS 2002 Telecommunications section (Appendix A). At a minimum this means that wireless communications must satisfy the requirements for telecommunications. The addition of wireless communications to a voting system adds to complexity both for security and testability, which currently cannot be justified.

Mobility
Mobility is not a necessary requirement to justify the use of wireless communications in voting systems, as it is not foreseen that voting devices will be moving during any phase of the voting process and still require connectivity.

Portability
Portability may present a convenience requirement for the use of wireless communications in voting systems, but not a necessity. It is foreseen that voting systems may be moved from one location to another between some phases of the voting process. For example moving the voting system(s) from the warehouse or storage facility to the polling location(s) and return. However means other than the use of wireless communications can accomplish any requirement for portability.

Wireless to replace cables or Wireless to reduce the number of cables or Wireless for portability or mobility.
Wireless to eliminate wires requires that the unit itself must not be powered by an electrical cord. Otherwise any requirement for the need to replace the

communications' cable is voided, since a power cord would be present. Thus any requirement to use wireless for the replacement of communications cabling shall be accompanied with the requirement that the voting device is also not connected via other cables, especially an AC power source cable.

Inclusion of wireless communications in a voting system is considered a convenience, however the added security risk may not justify its use. What follows now are recommendations which attempt to reduce the level of security risks, if wireless communications are to be used. The elimination of all security risks is not possible.

5.1. Attempting to secure wireless communications (general)

Securing wireless communications may be categorized in three ways: Organizational, Technical, and Physical. Each recommendation is marked as to whether it is a preventive, detective, or corrective measure. Also at least one reason is given for the recommendation.

5.1.1. Organizational recommendations

Organizational recommendations are considered outside the scope of the VSS 2002. However there is only so much that physical and technology recommendations can do without defining and ensuring that certain organizational procedures are followed. For example one can technically and physically require a capability for a password, however unless a person uses and changes the password appropriately, its ability to reduce risk is hollow.

5.1.2. Technical recommendations

Since these are general wireless communications recommendations, their applicability to some specific wireless technology may not be appropriate.

- Encryption (Preventive Measure)

All wireless communications shall be encrypted. This is to increase protection of the data being transferred over the air.

- Firewall (Preventive and Detective Measure)

All voting systems shall implement a firewall on a per device basis. This is to increase protection of the individual system from being accessed or compromised.

- No automatic discovery protocols shall be used to locate or connect to other wireless communication devices. (Preventive Measure)

Therefore a voting system shall have the capability to manually configure the identification required to be used to connect and to communicate with another wireless device.

- Spectrum usage (Preventive Measure)

To reduce the likelihood of interference the wireless technology chosen for implementation in a voting system should not use a frequency that is widely used for other devices that may be present in the expected environment.

- Frequency usage (Preventive Measure)

To reduce the likelihood of the voting system's wireless communication from being jammed, multiple frequencies should be available to use.

5.1.3. Physical recommendations

Implementing physical controls on the wireless communication signal is THE major issue. Of course, control of the physical device is also important, but that is true for any device, not just wireless devices.

- Identification of wireless technology (Preventive Measure)

Visual inspection (i.e., a label) of the wireless technology (e.g., radio frequencies (RF)) used must be available. This is to aid in the managing of wireless systems in order to reduce interference. [Note that even if a visual label is present indicating the type of wireless technology used by the particular wireless system/device, knowledge of whether the wireless communications devices will interoperate or interfere with each other is not necessarily known.]

- Identification of when wireless technology is in operation (Detective Measure)

Visual (or audio) indication for when the wireless technology is activated and operational shall be present. For the lowest level of security this will enable the ability to determine whether wireless communications devices are operational and/or activated for accessing a voting system.

- Control your signal strength

A device with wireless capabilities shall have capabilities to control the energy output of the wireless signal. This is an effort to reduce the coverage area or range of the wireless communications signal in order to lessen the eavesdropping risk. (Preventive Measure) It is also for the ability to increase signal strength as a method to decrease interference from other sources. (Corrective Measure)

- Reduce interference (Preventive Measure)

In order to reduce the level of interference that may disrupt or error the wireless communication, the following recommendations are made.

  - Any place where wireless communication devices are to be used shall not have any other wireless communications present that may interfere with the wireless voting system.
  - A site inspection shall be performed at the location where the wireless communications are to be operated.

  The results should show
  - what the current level of interference is. [Note that this is not an absolute measure, since there is no way of controlling all of the conditions effecting this measurement.]
  - what the expect coverage area or range of the proposed wireless voting system would be

  - Any place where wireless communication devices are to be used shall be shielded (Preventive Measure).

  The type of shielding is dependent upon the type of wireless used. For example if infrared is used in a room, shielding would be accomplished by ensuring that no light could get out of the area (i.e., no windows or open doors) Shielding for radio frequencies is not as easy.

5.2. Attempting to secure wireless communications (selected technologies)

Specific recommendations for specific wireless technologies are an endless process since there are always new or updated wireless technologies, as well as newly identifiable security risks and possible solutions. NIST Special Publication (SP) 800-48, “Wireless Network Security, 802.11, Bluetooth™[1] and Handheld Devices” examines, as the title states, two specific wireless technologies and one type of device. Its applicability to voting systems is a beginning. It is by no means a complete answer, especially since we know that both wireless technology’s security mechanisms have been compromised. This SP was published in 2002, however it is an example of just how quickly a technology and its security risk assessment become obsolete.

The newly released addendum, IEEE 802.11i, provides an alternative to the flawed Wired Equivalent Privacy (WEP) currently used in IEEE 802.11 wireless local area networks (WLANs). The Bluetooth technology continues to contain security risks, but markets them as features, such as bluejacking and bluesnarfing.

5.2.1. Guidance on Securing Existing Wireless Data Networks (IEEE 802.11 (Wi-Fi®[2]))

At a minimum:

- Existing wireless data networks shall upgrade to use the Wi-Fi protected access (WPA™) security protocol as soon as such upgrades are available.
- Until the WPA updates are available, all wireless data networks shall immediately enable wired equivalent privacy (WEP) protocol encryption. Non-WPA wireless data networks shall enable 128-bit WEP encryption. Non-WPA wireless data networks shall use virtual private network (VPN) software that will encrypt network communications and uniquely authenticate wireless users. This configuration will require the use of a firewall to block access by unauthenticated clients unless the VPN server provides similar functionality. Note, WEP encryption must be used in conjunction with VPN software, since encrypted VPN tunnels may not protect hackers from attacking other computers on the wireless network.

5.2.2. Recommendation on Securing Wireless Data Networks (IEEE 802.11 (Wi-Fi))

All implementations shall use Wi-Fi protected access 2 (WPA2™) and are FIPS 140-2 validated products.

[1] The Bluetooth word mark is owned by the Bluetooth SIG, Inc. Other trademarks and trade names are those of their respective owners. (C) Bluetooth SIG, Inc. 2003.

[2] Wi-Fi® is a registered trademarks of the Wi-Fi Alliance; and WPA™ and WPA2™ are trademarks of the Wi-Fi Alliance.

> WPA2 is the second generation of WPA security; providing enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard and is eligible for FIPS 140-2 compliance.

5.3. Wireless standards usage

Use wireless standards when available with the following caveats.

- Never use the first version of a wireless standard or specification because the standards or specifications are usually untested, loosely coherent, lack security, and almost 100% non-interoperable. Products built to the first version will, most likely, be incompatible with the next.
- Never use the first implementation of a wireless communications device or systems as it has no experience in areas outside its production design facilities.

  > Case in point the Bluetooth Special Interest Group (BSIG), which has released a new version of their specification almost yearly, invalidating the previous version with each revision. The security was quickly and easily compromised in the first version and, similarly, the next. IEEE 802.15.3 and 802.15.4 standards were published even though there existed outstanding issues and began collecting and revising text for the next version.
- Obsolescence of information technology is rampant, wireless communications are no exception. Therefore unless one has the resources to continually review, revise, secure, and test the inclusion of wireless communications into a voting system and has a solid justification for its use, one should not include wireless communications in a voting system.

  > Cellular technology provides wireless communications, but has an industry life duration of one year. For a voting system that uses cellular technology this means that approximately every year the voting system will need to be replaced or at least the wireless part will need to be replaced. For a formal validation of the voting system, this means another test or set of tests every year.

5.4. Testing wireless communications

Testing of any wireless technology shall be through the same means as the when under normal operations. It cannot be through a special testing port, messages, interface, or mode. This requirement is made to ensure that the real implementation system is tested and not an implementation designed for testing only. The Bluetooth technology provisioned a special port, interface, and mode along with specific messages and codings just for testing implementations for compliance or conformance.

References

Wireless LAN Technology issues and strategies
Peter T. Davis, Craig R. McGuffin
TK 5105.7.D388-1995

Secure Broadcast Communications in Wired and Wireless Networks
Adrian Perrig, J.D. Tygar
Kluwer Academics Publishers
TK5012.85.P47-2003

Handbook of Mobile Radio Networks
Sami Tabbare
TK6570.M6T33-2000

Narrowband Land-mobile Radio Networks
Jean-Paul
TK6570.M6L56-1993

802.11 Security
TK5105.59.P68-2003

NIST Construction Automation Program Report No. 3: Electromagnetic Signal Attenuation in Construction Materials.
Stone, W. C.
NIST Internal Report (NISTIR) 6055; 199 p. October 1997.

Wireless Network Security 802.11, Bluetooth and Handheld Devices.
Karygiannis, T. and Owens, L.
Special Publication (SP) 800-48, November 2002

Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001 (change notice 12/03/2002)

Federal Information Processing Standards (FIPS) Publication 197, *Advanced Encryption Standard (AES)*, November 26, 2001

IEEE Standard for Information technology--Telecommunications and information exchange between system--Local and metropolitan area networks (LAN/MAN) Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications--Amendment 6: Medium Access Control (MAC) Security Enhancements, June 24, 2004

Appendix A Update to VSS2002 Volume 1, section 5, Telecommunications

This appendix contains notes against the text from VSS2002 Volume 1, section 5, Telecommunications, that will need to be addressed when a final decision is made to allow or prohibit wireless communications.

5 Telecommunications

5.1 Scope

This section contains the performance, design, and maintenance characteristics of the telecommunications components of voting systems and the acceptable levels of performance against these characteristics. For the purpose of the Standards, telecommunications is defined as the capability to transmit and receive data electronically using hardware and software components over distances both within and external to a polling place.

> [Note that with this definition wireless is implicitly included. Therefore there is no need to explicitly define it. If wireless communications is to be prohibited, then this definition has to be changed.]

The requirements in this section represent acceptable levels of combined telecommunications hardware and software function and performance for the transmission of data that is used to operate the system and report election results. Where applicable, this section specifies minimum values for critical performance and functional attributes involving telecommunications hardware and software components.

This section does not apply to other means of moving data, such as the physical transport of data recorded on paper-based media, or the transport of physical devices, such as memory cards, that store data in electronic form.

Voting systems may include network hardware and software to transfer data among systems. Major network components are local area networks (LANs), wide area networks (WANs), workstations (desktop computers), servers, data, and applications. Workstations include voting stations, precinct tabulation systems, and voting supervisory terminals. Servers include systems that provide registration forms and ballots and accumulate and process voter registrations and cast ballots.

Desirable network characteristics include simplicity, flexibility (especially in routing, to maintain good response times) and maintainability (including availability, provided primarily through redundancy of resources and connections, particularly of connections to public infrastructure).

A wide area network (WAN) public telecommunications component consists of the hardware and software to transport information, over shared, public (i.e., commercial or governmental) circuitry, or among private systems. For voting systems, the telecommunications boundaries are defined as the transport circuitry, on one side of *which exists the public telecommunications infrastructure, outside the control of voting system supervisors. On the other side of the transport circuitry are the local area network (LAN) resources, workstations, servers, data and applications controlled by voting system supervisors.*

Local area network (LAN) components consist of the hardware and software infrastructure used to transport information between users in a local environment, typically a building or group of buildings. Typically a LAN connects workstations, perhaps with a local server.

An application may be a single program or a group of programs that work together to provide a function to an end user, who may be a voter or an election administrator. Voter programs may include voter registration, balloting, and status checking. Administrator programs may include ballot preparation, registration for preparation, registration approval, ballot vetting, ballot processing, and election processing.

This Section is intended to compliment the network security requirements found in Volume I Section 6, which include requirements for voter and administrator access, availability of network service, data confidentiality, and data integrity. Most importantly, security services will restrict access to local election system components from public resources, and these services will also restrict access to voting system data while it is in transit across public resources. (This is corollary to voting supervisors controlling local election systems and not assuming control over public resources.)

5.1.1 Types of Components

This section addresses telecommunications hardware and software across a broad range of technologies including, but not limited to:

- *Dial-up communications technologies:*
  - *Standard landline;*
  - *Wireless;*
  - *Microwave;*
  - *Very Small Aperture Terminal (VSAT);*

    [Note the previous three bulleted items are all wireless communications. The first item would need to be refined so that it is clear what is meant by the term, wireless. If wireless is decided to be prohibited, then all three items must be deleted.]
  - *Integrated Services Digital Network (ISDN); and*
  - *Digital Subscriber Line (DSL);*
- *High-speed telecommunications lines (public and private):*
  - *FT-1, T-1, T-3;*
  - *Frame Relay; and*
  - *Private line;*
- *Cabling technologies:*
  - *Universal Twisted Pair (UTP) cable (CAT 5 or higher);*
  - *Ethernet hub/switch; and*
  - *Wireless connections (Radio Frequency (RF) and Infrared);*

[Note this item restricts wireless communications to include radio frequency and infrared. A decision must be made as to whether to keep this limitation, to expand it, or to delete it.]

¨ *Communications routers;*

¨ *Modems, whether internal and external to personal computers, computer servers, and other voting system components (whether installed at the polling place or central count location);*

¨ *Modem drivers, dial-up networking software;*

¨ *Channel service units (CSU)/Data service units (DSU) (whether installed at the polling place or central count location); and*

¨ *Dial-up networking applications software.*

5.1.2 Telecommunications Operations and Providers

This section applies to voting-related transmissions over public networks, such as those provided by regional telephone companies and long distance carriers. This section also applies to private networks regardless of whether the network is owned and operated by the election jurisdiction.

For systems that transmit official data over public networks, this Section applies to telecommunications components installed and operated at settings supervised by election officials, such as polling places or central offices. These standards apply to:

¨ *Components acquired by the jurisdiction for the purpose of voting, including components installed at the poll site or a central office (including central site facilities operated by vendors or contractors); and*

¨ *Components acquired by others (such as school systems, libraries, military installations and other public organizations) that are used at settings supervised by election officials, including minimum configuration components required by the vendor but that the vendor permits to be acquired from third party sources not under the vendor's control (e.g., router or modem card manufacturer or supplier)*

5.1.3 Data Transmissions

These requirements apply to the use of telecommunications to transmit data for the preparation of the system for an election, the execution of an election, and the preservation of the system data and audit trails during and following an election. While this section does not assume a specific model of voting system operations and does not assume a specific model for the use of telecommunications to support such operations, it does address the following types of data, where applicable:

¨ *Voter Authentication: Coded information that confirms the identity of a voter for security purposes for a system that transmits votes individually over a public network;*

¨ *Ballot Definition: Information that describes to a voting machine the content and appearance of the ballots to be used in an election;*

¨ *Vote Transmission: For systems that transmit votes individually over a public network, the transmission of a single vote within a network at a polling place and to the county (or contractor) for consolidation with other county vote data;*

¨ Vote Count: Information representing the tabulation of votes at any level within the control of the jurisdiction, such as the polling place, precinct, or central count; and
¨ List of Voters: A listing of the individual voters who have cast ballots in a specific election.

Additional data transmissions used to operate a voting system in the conduct of an election, but not explicitly listed above, are also subject to the standards of this section. For systems that transmit data using public networks, this section applies to telecommunications hardware and software for transmissions within and among all combinations of senders and receivers indicated below:

¨ Polling places;
¨ Precinct count facilities; and
¨ Central count facilities (whether operated by the jurisdiction or a contractor).

5.2 Design, Construction, and Maintenance Requirements

Design, construction, and maintenance requirements for telecommunications represent the operational capability of both system hardware and software. These capabilities shall be considered basic to all data transmissions.

5.2.1 Accuracy

The telecommunications components of all voting systems shall meet the accuracy requirements of Section 3.2.1.

5.2.2 Durability

The telecommunications components of all voting systems shall meet the durability requirements of Section 3.4.2.

5.2.3 Reliability

The telecommunications components of all voting systems shall meet the reliability requirements of Section 3.4.3.

5.2.4 Maintainability

The telecommunications components of all voting systems shall meet the maintainability requirements of Section 3.4.4.

5.2.5 Availability

The telecommunications components of all voting systems shall meet the availability requirements of Section 3.4.5.

5.2.6 Integrity

For WANs using public telecommunications, boundary definition and implementation shall meet the following requirements.

a. Outside service providers and subscribers of such providers shall not be given direct access or control of any resource inside the boundary;
b. Voting system administrators shall not require any type of control of resources outside this boundary. Typically, an end point of a telecommunications circuit

will be a subscriber termination on a Digital Service Unit/Customer Service Unit (DSU/CSU) (though the precise technology may vary, being such things as cable modems or routers). Regardless of the technology used, the boundary point must ensure that everything on one side is locally configured and controlled while everything on the other side is controlled by an outside service provider; and

c. The system shall be designed and configured such that it is not vulnerable to a single point of failure in the connection to the public network causing total loss of voting capabilities at any polling place.

5.2.7 Confirmation

Confirmation occurs when the system notifies the user of the successful or unsuccessful completion of the data transmission, where successful completion is defined as accurate receipt of the transmitted data. To provide confirmation, the telecommunications components of a voting system shall:

d. Notify the user of the successful or unsuccessful completion of the data transmission; and

e. In the event of unsuccessful transmission, notify the user of the action to be taken.

Appendix B Update to VSS2002 Volume 1, section 6, Security Standards

This appendix contains an additional subsection for the current version of VSS2002 Volume 1, section 6, Security Standards that includes wireless communications in a private setting, since wireless used in a public setting are already covered by the telecommunications section of VSS 2002 Volume I. A significant part, which is no included, is the operational procedures during any phase of the voting process or system.

6.7 Security for Transmission of Official Data Over Wireless Communications Networks (Private)

DRE systems that transmit data over wireless communications face additional security risks that are not present in other DRE systems telecommunications or data networks. This section describes standards applicable to DRE systems that use wireless communications networks (private).

6.7.1 General Security Requirements for Systems Transmitting Data Over Wireless Communications Networks

All systems that transmit data over wireless communications networks shall:

a. Preserve the secrecy of a voter's ballot choices, and prevent anyone from violating ballot privacy;
b. Employ digital signature for all communications between the vote server and other devices that communicate with the server over the wireless network; and
c. Require that at least two authorized election officials activate any critical operation regarding the processing of ballots transmitted over a wireless communications network takes place, i.e. the passwords or cryptographic keys of at least two employees are required to perform processing of votes.

6.7.2 Voting Process Security for Casting Individual

Ballots over a Wireless Communications Network Systems designed for transmission of communications over wireless networks shall meet security standards that address the security risks attendant with the casting of ballots from poll sites controlled by election officials using voting devices configured and installed by election officials and/or their vendor or contractor, and using in-person authentication of individual voters.

6.7.2.1 Documentation of Mandatory Security Activities

Vendors of systems that cast individual ballots over a wireless communications network shall provide detailed descriptions of:

a. All activities mandatory to ensuring effective system security to be performed in setting up the system for operation, including testing of security before an election; and
b. All activities that should be prohibited during system setup and during the time frame for voting operations, including both the hours when polls are open and when polls are closed.

6.7.2.2 Capabilities to Operate During Interruption of Wireless Communications Capabilities

These systems shall provide the following capabilities to provide resistance to interruptions of wireless communications service that prevent voting devices at the poll site from communicating with external components via wireless communications:

a. Detect the occurrence of a wireless communications interruption at the poll site and switch to an alternative mode of operation that is not dependent on the connection between poll site voting devices and external system components;
b. Provide an alternate mode of operation that includes the functionality of a conventional DRE machine without losing any single vote;
c. Create and preserve an audit trail of every vote cast during the period of interrupted communication and system operation in conventional DRE system mode;
d. Upon reestablishment of communications, transmit and process votes accumulated while operating in conventional DRE system mode with all security safeguards in effect; and
e. Ensure that all safeguards related to voter identification and authentication are not affected by the procedures employed by the system to counteract potential interruptions of telecommunications capabilities.