EAC RESEARCH AREAS FOR THE TGDC VVSG RECOMMENDATIONS

January, 2009

National Institute of Standards and Technology (NIST)

NIST Voting Team

OVERVIEW AND SUMMARY

On August 31, 2007 NIST delivered the Technical Guidelines Development Committee (TGDC) Voluntary Voting System Guidelines (VVSG) Recommendations to the Election Assistance Commission (EAC). The EAC began a public comment period and conducted meetings with the EAC's Board of Advisors and Standards Board. The EAC identified six areas of research related to the VVSG in response to resolutions passed by those boards. The EAC asked NIST to conduct research on feasibility and scope of impact in these six areas.

This document contains reports on the research conducted by NIST.

The six areas identified by the EAC are:

1. Possible alternatives to the requirement of Software Independence;
2. Possible standards for ballot on demand systems;
3. Potential impact of the VVSG on vote by phone systems;
4. A feasibility study of the ramifications of the EAC separately testing and certifying components of a voting system, and requirements for interoperability between systems and system components;
5. Impact of early voting and vote centers on the VVSG; and
6. Identification of "goal level requirements" in the VVSG and developing alternatives.

Each report contains a summary, explanatory details and a section on next steps, where applicable.

Note: the VVSG is herein referred to as the “VVSG-NI” for “VVSG-next iteration.”

AREA 1: POSSIBLE ALTERNATIVES TO THE REQUIREMENT OF SOFTWARE INDEPENDENCE

Wording from the EAC: "Develop possible alternatives to the requirement of Software Independence, which is included in the TGDC draft recommendations. These alternatives should, of course, retain the focus on security, verifiability, and auditability present in the current document. In providing the possible alternatives, research should be conducted on what changes would need to be made to the TGDC draft recommendations in order [to] use that alternative in the next iteration of the VVSG."

SUMMARY

This research proposes three alternatives to Software Independence (SI), but all require significant research and prototyping before requirements could be written for the VVSG-NI. In summary, one possible strategy for changing the VVSG-NI to permit alternatives to SI would be to replace the overarching SI requirements with a requirement for rigorous auditability, and to list SI as one method for achieving auditability. There could be others, such as:

1. End-to-End (E2E) systems – prototypes and a product exist today, but further research and development is needed. There is much interest from the academic community in developing further prototypes.

2. Independent Verification (IV) systems – included as informative text in the VVSG 2005; no products exist today.

3. Standard audit port for voting systems – a superset of IV; no products exist today, but there are some similar products that could be used to draw upon for requirements.

Also, the SI requirement would no longer apply to Innovation Class submissions.

Each of the alternatives to SI has various associated pros and cons, which are listed in the sections below that compare the different alternatives. The advantages of replacing the overarching SI requirement with a requirement for rigorous auditability include that the VVSG-NI would then have a structure in place to accommodate different approaches to auditability other than purely SI. As different alternatives are developed and vetted, they could be added as modules of requirements to the VVSG-NI. The advantages of removing the SI restriction from the Innovation Class include that manufactures are freer to design new approaches that would still meet the auditability requirements but that may not necessarily conform to SI or other alternatives. Accessibility and usability requirements will still apply and must also be considered for any new approaches.

The EAC may wish to consider convening a focused research effort to explore these alternatives, possibly holding several workshops whose purpose would be to collect and highlight key research and to work towards a research and development plan for prototypes and other implementations. Such an approach could help determine which alternatives are most viable and could result in prototype products and, at some point, actual requirements that could be added as modules to the VVSG-NI.

DEFINITIONS

This section provides the definitions of several terms that will be used throughout this report and serves as background, scope, and context for the discussion of alternatives to software independence.

- ***Voting system:*** Equipment (including hardware, firmware, and software), materials, and documentation used to define elections and ballot styles, configure voting equipment, identify and validate voting equipment configurations, perform logic and accuracy tests, activate ballots, capture votes, count votes, reconcile ballots needing special treatment, generate reports, transmit election data, archive election data, and audit elections.

- ***Auditability:*** Quality of a voting system or device such that that any error in its recording of votes or vote totals, whether randomly occurring or maliciously induced, is detectable.

- ***Software Independence (SI):*** Quality of a voting system or device such that a previously undetected change or fault in software cannot cause an undetectable change or error in election outcome.

- ***Independent Voter Verifiable Record (IVVR):*** Record produced by an IVVR vote capture device supporting voter verification (e.g. VVPAT, EBM). The record contains minimally a summary of the electronic Cast Vote Record. One example of an independent voter verifiable record is a voter verifiable paper record.

- ***Independent Voter Verifiable Record System (IVVR System):*** A voting system that achieves software independence by using Independent Voter-Verifiable Records (IVVR).

- ***Independent Verification systems (IV):*** Multi-component voting system architectures that have an additional hardware component to serve as a "witness" (by monitoring and recording) to a DRE's behavior in such a way that an undetectable change or error in a cast ballot can occur only if both the DRE and the additional hardware component fail. Voting system architectures with more than a single additional hardware component connected to the DRE also fall under the IV category.

- ***End-to-End systems (E2E):*** Voting systems in which the voter can verify that their vote is counted as cast. This typically involves publication of the (anonymized) votes through a public medium (such as a newspaper or public website).

MAKING AUDITABILITY THE CENTRAL SECURITY REQUIREMENT

The overall strategy behind the alternatives to SI is to make auditability, rather than SI, the central security property requirement of the voting equipment. Currently, voting systems that conform to the VVSG must be SI, even if they require use of the Innovation Class conformance process, which has not yet been specified. The VVSG-NI contains a high-level requirement for SI, and then contains several lower-level audit-related requirements that in effect state that the SI requirement can be achieved via auditability (see Figure 1).

An alternative view is that SI could be one among several possible ways of achieving auditability, and therefore auditability should be the high-level requirement, with SI (or voting systems that are SI) being a lower-level requirement. Voting systems proposed under the Innovation Class conformance process would not necessarily have to be SI, but must meet the higher-level requirement of auditability (see Figure 2).

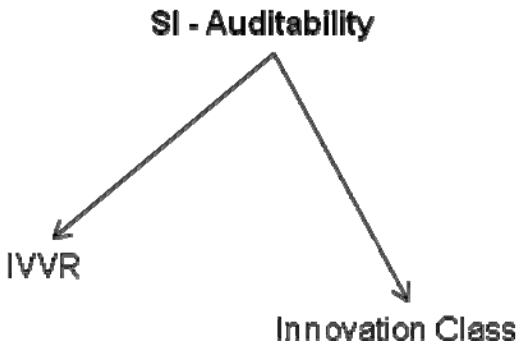

Figure 1: Current structure of SI requirement in VVSG-NI

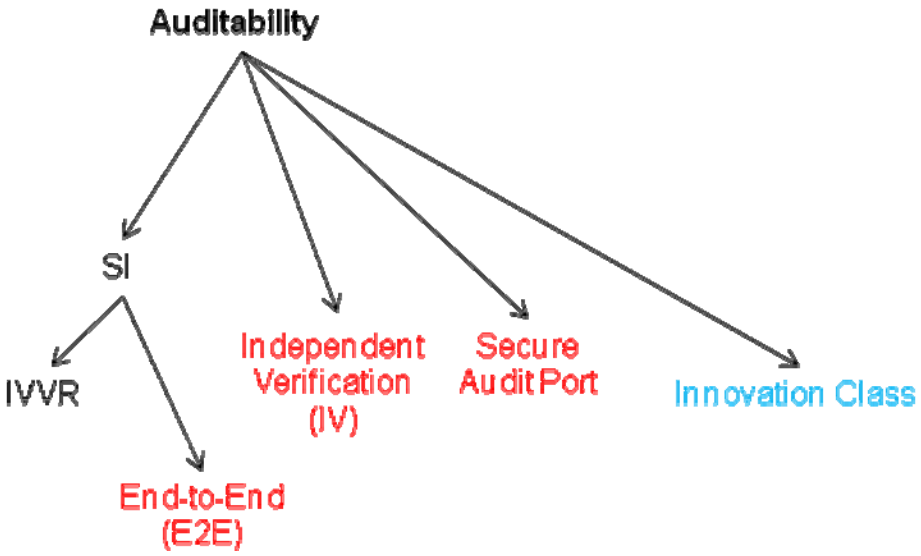

Figure 2: Proposed auditability structure

Accordingly, the VVSG-NI could have one or more high-level auditability requirements that essentially demand that any error, whether randomly occurring or maliciously induced, is detectable (error is defined essentially as an incorrect vote total result), e.g.,

> All voting systems SHALL be auditable.

NOTE: It would have to be clear, however, that the methods for voting systems to be auditable must be highly reliable and robust, and that today's DRE voting systems would not meet this requirement.

Following the auditability requirement would then be requirements that allow voting systems to achieve auditability e.g., voting systems that are SI (such as IVVR voting systems), and, if developed, voting systems that are approved alternatives to SI. Lastly, as stated already, the current SI restriction on the Innovation Class would be removed.

ALTERNATIVES TO SI

The following sections briefly describe voting system approaches that are alternatives to SI.

END-TO-END VOTING SYSTEMS

End-to-End (E2E) voting systems often involve a physical, e.g., paper receipt that the voter can use to verify, during the process of voting, whether his or her electronic ballot was captured correctly. The receipt does not show how the voter voted. The electronic ballots are encrypted and copies are stored on an electronic bulletin board at a public website so that the voter, using the same receipt, can verify that his or her ballot was counted in the election totals.

By definition, E2E voting systems achieve a very strong form of auditability that allows voters to verify that their votes were counted as cast. However, most E2E systems rely, to some degree, on the accuracy of some software to achieve audibility. Because of this, there are varying opinions regarding whether or not E2E voting systems can be SI. The answer may depend on the precise interpretations of SI and E2E. This document tentatively assumes SI is an explicit requirement of E2E voting systems (See Figure 2). However since E2E voting systems are auditable, whether or not E2E voting systems are SI is not a major security concern. For the purposes of this document, E2E voting systems are considered an "alternative to SI" because they do not, in principle, require counting and storing paper records.

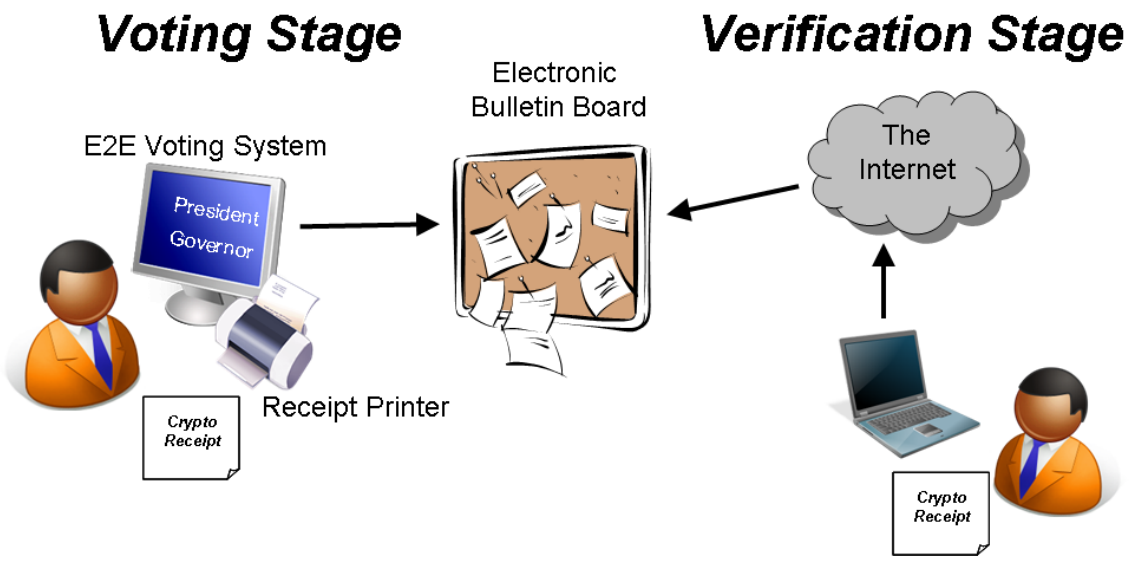

Figure 3: Example of an End-to-End System Architecture

INDEPENDENT VERIFICATION VOTING SYSTEMS

Another type of auditable electronic voting system, known as an Independent Verification (IV) system, would record and store voter ballot selections on multiple independent voting system components. Such systems would typically consist of a vote capture device connected to a monitoring device. The monitoring device would store an independent record of the election and be capable of detecting flaws in the vote capture device. It is important to note that an IV system is not merely a vote capture device with redundant storage. The system would need to provide some assurance that the monitoring device is recording the correct ballot choices, and that assurance must be independent from the vote capture device. One example of an IV system discussed in the 2005 VVSG uses a split-process architecture. The voter makes ballot selections on a vote capture device, which passes the selections to a monitoring device. The monitoring device displays those selections to the voter for verification purposes.

IV systems allow purely electronic audit records. A signed electronic record of each cast ballot could be issued by the vote capture device and stored by an independent monitoring device. Compared to paper records, digitally signed electronic records can be easily replicated and verified in an automated fashion. In principle, these records could be published so anybody could verify the election counts. The concept of "custody independence" (CI) has been proposed as a security principle complementary to SI. Whereas SI addresses the risk of inaccurate or fraudulent voter records being created at the vote casting stage, CI addresses the risk of failure or sabotage of the chain of custody mechanisms that ensure that the votes cast are the same as the votes counted.

However, IV systems are not necessarily SI and may rely on the software on the system components. While SI systems must be capable of detecting any flaw in software, IV systems only detect flaws if at least one system component is functioning appropriately. Successful attacks against all voting system components may be capable of causing an undetectable change to an election outcome.

Figure 4: IV System using a Split-Process Architecture

STANDARD AUDIT PORT APPROACH TO VOTING SYSTEMS

The current draft of the VVSG-NI envisions voting devices as single, unified devices capable of meeting all of the VVSG-NI requirements for a particular class. An alternative, more flexible, approach would be to design DRE-based vote capture devices with an audit port that could be connected, as needed, to an audit device (however, systems relying on the functionality provided by an audit device would likely need to be certified with the audit device. The issue of testing and certifying individual components is discussed in Area 4.)

An audit port would allow verification devices to be connected to a DRE-based vote-capture device to obtain electronic audit records without the ability to modify the voting system software and audit records. The primary function of DRE-based vote capture device could be to provide an accessible user interface for the voter to make ballot selections. The verification device could implement some or all of the specific functionality required for a particular class (such as producing a VVPR or a cryptographic receipt, or serving as an independent verification device). For example, a printer could be connected to a voting device using the audit port, thus creating an IVVR voting system. This approach is flexible, and could make it possible for jurisdictions to move to new kinds of voting systems while reusing previously purchased devices (as long as those devices contain the audit port). For instance, a jurisdiction could replace a printer verification device with an independent verification device, thus creating an IV system.

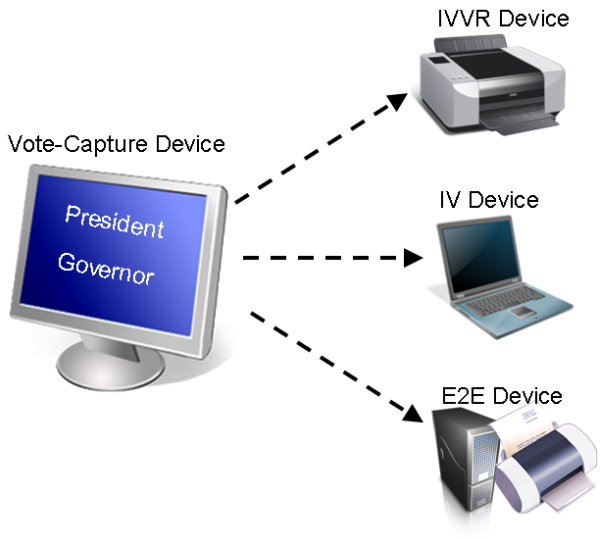

Figure 5: Audit Port Examples

COMPARISON OF APPROACHES

Creating a separate path to conformance and developing requirements for E2E and IV voting systems involves largely untested technologies. This significantly impacts the amount of work/research required for completing the VVSG-NI. This section briefly discusses the issues related to creating a separate path to conformance and developing requirements for E2E voting systems, IV voting systems, and voting systems with an audit port.

E2E SYSTEMS:

The pros for E2E voting systems include that election records could be all electronic and voters could have confidence that their votes would be recorded correctly and included in the final tally. Among the alternatives that have been contemplated in this document, E2E voting systems possess the best security properties and would be a significant achievement if deployed. There is significant academic interest in producing E2E voting systems.

The cons for E2E voting systems include that significant disagreements on important details concerning E2E technology, such as the necessary level of detail in requirements, need to be resolved. Although some have said that requirements for E2E would be straightforward to write, NIST's experience dictates a more cautious view. The process of resolving these issues at the Technical Guidelines Development Committee (TGDC) level could be lengthy and would significantly impact the workload involved in drafting the VVSG-NI requirements.

In addition, usability and accessibility studies are urgently needed for E2E voting systems. All proposed E2E systems involve changes in (a) the way the vote is cast, (b) the tally computed, and (c) the result made public.

There is no way of predicting how the public would receive E2E voting systems and what kinds of error rates are inherent to the technology. Furthermore, it is conceivable that usability studies would lead to modifications in security requirements. The lack of usability and accessibility studies of E2E voting systems makes it difficult to provide a timeframe for the development of requirements for such systems.

IV SYSTEMS:

The pros for IV voting systems include that election records could be all electronic and voters could have confidence that their votes would be recorded correctly. Conceivably, different types of IV systems could be created that do not involve verification of two records, such as the witness system that essentially records a voter's verification of the electronic record. Depending upon how well the interface between the two devices could be specified, vendors could be relatively free to innovate with different approaches.

The cons for IV voting systems include that the basic system architecture of an IV voting system would be significantly different than current electronic voting systems. There is still significant disagreement over the necessary system architecture and requirements to achieve a secure voting system. Many of these disagreements are related to the way multiple components of a single IV system should interact with one another.

Thus there are significant uncertainties regarding the timeframe for completion of this task, but we expect the level of effort to be comparable to that for E2E systems.

STANDARD AUDIT PORT:

The pros for voting systems with a standard audit port include that a real-time accounting of a voting session could be captured and exported for audit. The stream of information could use a standard language such as EML (Election Markup Language). The information obtainable through the audit port could be used for purposes other than enhancing auditability (such as enhancing accessibility, or producing high-quality summary screens in order to reduce voter error). This information may be useful for identifying certain types of attacks, such as ballot presentation attacks, that would be difficult to detect in other voting systems.

The cons for voting systems with an audit port include, like IV, that the basic system architecture would be significantly different than current electronic voting systems. Significant research might be involved in writing requirements for an audit port. The issues that would need to be addressed include (but may not be limited to):

- Defining the election data and the standard format of the election data fields that would be exported through the audit port;
- Determining if EML (or another markup language) is sufficient to express the data defined in the previous point;
- Reviewing and enhancing requirements (from the VVSG-NI and 2005 VVSG) for electronic audit records;
- Researching the possible security vulnerabilities introduced by an audit port.

Considerable changes to the conformity assessment program would be needed to accommodate audit port testing. Interoperability testing would need to be incorporated into the testing program, which is significantly different than the functional, reliability, security and usability testing currently in the program.

As with IV, there are significant uncertainties regarding the timeframe for completion of this task, but it would be expected to involve a similar amount of effort as with E2E systems.

NEXT STEPS

The EAC may wish to consider convening a focused research effort to explore these alternatives, possibly holding several workshops whose purpose would be to collect and highlight key research and to work towards a research and development plan for prototypes and other implementations. Such an approach could help determine which alternatives are most viable and could result in prototype products and, at some point, actual requirements that could be added as modules to the VVSG-NI.

AREA 2: STANDARDS FOR BALLOT ON DEMAND SYSTEMS

Wording from the EAC: "Developing standards for Ballot on Demand systems. This research should begin with the study of the feasibility of including Ballot on Demand standards in the VVSG, e.g., are election official needs adequately represented in existing vendor ballot on demand systems or whether more research would need to be conducted with election officials to better understand their needs."

SUMMARY

The main issue addressed by this research is whether Ballot on Demand (BOD) requirements can, at this time, be defined and added to the VVSG-NI (Ballot on Demand is a device or system in which ballots can be printed "on demand" rather than produced in advance).

At this time, there is no consensus among vendors or election officials as to the specifics of BOD, what it integrates with, how it works, and what problems it solves. Therefore, before requirements for the VVSG-NI could be written, more research is needed as to what BOD products or prototypes already exist and how that may differ from what election officials believe they need. In performing this research, there are a number of issues in core requirements, security, and human factors that must be addressed.

A reasonable next step would be for the EAC to convene a focused research effort to address these issues. This research effort could include working groups and workshops, and could result in a requirements specification for ultimate inclusion in the VVSG-NI.

ISSUES REGARDING BOD

Questions regarding Ballot on Demand capabilities (BOD) in the VVSG-NI first arose during election official reviews of the VVSG-NI draft in preparation for the December 2007 meetings of the Standards Board and Board of Advisors. NIST initiated a thread on a mailing list of election officials selected from the two boards to gather more background information on this technology. The responses from the election officials, together with information gleaned from searching the Internet and subsequent discussions with individuals, revealed a diversity of beliefs regarding the specifics of BOD, what it integrates with, how it works, and what problems it solves. Each of the following has been cited as exemplary of BOD at one time or another:

1. A dedicated EMS application running in the polling place is used by election officials on location to produce additional ballots in response to emergencies such as (1) the ballots prepared in advance run out; (2) as a back-up voting mechanism in case the DREs won't work; (3) as an accommodation for voters who specifically want or need a paper ballot instead of a DRE.

2. A dedicated application, possibly integrated with an electronic pollbook and/or registration database, prints out a ballot of the correct ballot style as each voter is checked in, based on each voter's registration information. No ballots are prepared in advance. May be of particular use in vote centers for early voting.

3. BOD = Electronic Ballot Printer (per the VVSG-NI definition), an Electronically-assisted Ballot Marker which integrates the BOD functionality. One does not need to have a blank ballot of the correct ballot style prepared in advance; the device activates the correct style of ballot, collects the votes, and prints the completed ballot (both ballot style information and votes) onto blank paper. No electronic record of the votes is retained by the device.

4. A DRE has a BOD feature as a kind of add-on whereby it can send an activated ballot to a printer instead of displaying it on the touchscreen.

    a. If the ballot is not filled in with votes, then this is just another way of implementing the BOD functionality in #1 and #2.

    b. However, if the ballot is filled in with votes collected via the touchscreen interface, then this is a combination of the DRE and EBP concepts defined in the draft VVSG-NI, one that potentially retains an electronic record of votes in addition to producing the paper ballot and could produce a separate electronic tabulation of votes parallel to the tabulation of the paper ballots. This raises lots of issues.

5. Ballots are produced "on demand" by trained staff at remote locations for overseas voters. This is a significantly different use case but possibly the same equipment as discussed above.

6. Voters can print out legal absentee ballots on their personal PCs at home. This is a significantly different use case AND significantly different equipment.

The one clear point of commonality is that, by definition, BOD means that ballots will be printed "on demand" rather than produced in advance. Beyond that, the specific details are highly variable. In particular, the consequences for voting system security and privacy would need to be researched and codified.

NEEDED INFORMATION

From the above, it seems clear that focused research on BOD requirements is needed before VVSG-NI requirements could be written. NIST would need to obtain clear information on the following:

1. What BOD products already exist, what do they integrate with, how do they work, and what problems do they solve? NIST's research uncovered some high-level information on existing products by Premier ("Ballot On Demand") and Hart ("Ballot Now"), but it would be preferable to obtain the most specific, recent, traceable, and complete information from the manufacturers.

2. What BOD products do election officials want, what must they integrate with, how must they work, and what problems must they solve? E.g., if election officials strongly demand a BOD product that integrates

directly with an electronic pollbook and/or registration database, then this possibility must be addressed by the VVSG-NI one way or another, even if no existing products currently do this.

NEXT STEPS

A reasonable next step is for the EAC to convene a focused research effort to address the issues described in this report and to collect the needed information before requirements writing could be considered. This research effort could include the use of mailing lists, working groups, and meetings, and workshops, and could result in a requirements specification for ultimate inclusion in the VVSG-NI. Involvement would be needed from the vendor community, test labs, election officials, and experts in core requirements, security, and human factors.

AREA 3: POTENTIAL IMPACT OF THE VVSG-NI ON VOTE BY PHONE SYSTEMS

Wording from the EAC: "Producing a study on the potential impact the proposed VVSG-NI would have on Vote by Phone systems. This research should address questions that have been raised as to whether existing requirements in the VVSG-NI, as written, would prohibit Vote by Phone systems, and if so, what changes would be required to permit them."

SUMMARY

There are two main issues that are addressed by this research:

1. Whether existing vote-by-phone (VBP) implementations could conform as an accessible voting station (Acc-VS) under the VVSG-NI, and

2. Whether a VBP implementation for general-purpose voting would meet relevant requirements in the VVSG-NI.

The first issue, the VBP used as an ACC-VS, is impacted by an interpretation of the Help America Vote Act (HAVA), reflected in the VVSG-NI's requirements, that essentially requires the Acc-VS to accommodate all applicable disabilities, e.g., blindness, low vision, poor dexterity, and lack of mobility[1]. Consequently, existing audio-only implementations, such as the VBP used in Vermont, would not conform. Two approaches could be considered, with associated pros and cons:

a. Create a VBP with additional capabilities to address all the accessibility requirements, which has the benefit of not requiring a reinterpretation of HAVA; all voters regardless of disability could use the VBP system. However, such a system would be costly.
b. Modify this interpretation of conformance to allow different voting stations and devices addressing different specific disabilities to be certified and provide guidance as to how a polling location would use these systems to meet the requirements of HAVA.

This issue also brings up the question of the usability of the VBP interface and whether additional requirements based on the best practice in design of Voice User Interfaces should be developed for the VVSG-NI.

The second issue, the VBP used for general-purpose voting, is also problematic. There would be many other modifications to the VVSG-NI that include security and functionality requirement changes and additions. Most

[1] HAVA says, The voting system shall--

(A) be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters;

(B) satisfy the requirement of subparagraph (A) through the use of at least one direct recording electronic voting system or other voting system equipped for individuals with disabilities at each polling place;

notably, the security changes would require encryption to be used between the telephone and back-end systems. An audio-only VBP is also not suitable for some voters who normally would use the general visual voting station (not the ACC-VS) such as those who are deaf or who have various cognitive problems.

Adding requirements for VBP would require, conservatively, one or more years. VBP may be considered as a form of remote voting and thus "different enough" to warrant not intermingling VBP requirements with the requirements for precinct-based equipment in the VVSG-NI. Otherwise, the requirements for precinct-based equipment would have to be modified or weakened substantially to accommodate VBP. An alternative would be to place requirements for VBP in a separate voting standard or perhaps in a special appendix of the VVSG-NI dedicated to remote voting equipment.

VBP GENERAL ARCHITECTURE

Vote-by-phone (VBP) is voting system in which the primary voter interface is a conventional telephone. In addition, the VBP system has a back-end system that captures and stores voter choices that are submitted using a conventional telephone. Note, this type of voting system represents a remote voting system since the voter and the system that stores a voter's choices are physically separated.

The following figure is provided to illustrate the general architecture and components of a VBP system.

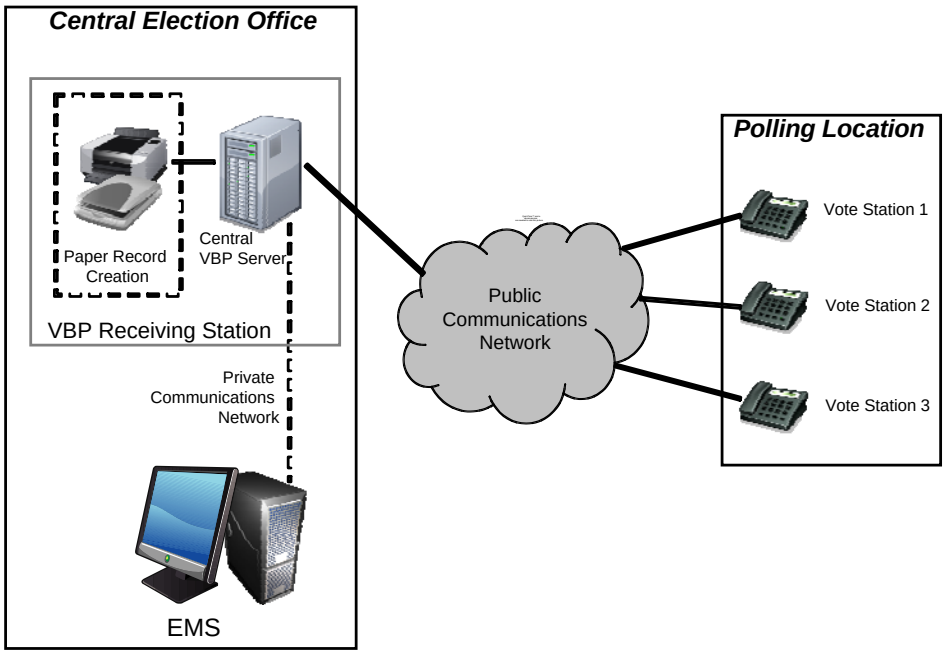

Figure 6: Vote-by-phone general architecture

Figure 6 shows that there are two physically separated locations: (1) the polling location and (2) the Central Election Office. In the polling location, there are voting stations with a telephone interface used by the voters. In the Central Election Office, there is the VBP receiving station that captures and stores the voter's choices. The VBP receiving station may optionally create a paper record of each voter's selections. In addition, the Central Election Office has an election management system (EMS) to configure the VBP receiving station and collect election results. Between the polling place and Central Election Office, a public communication network is used to carry the voting information between the locations.

TELEPHONE VOTE STATION (TELEPHONE):

In the polling location, there are voting stations with a telephone interface used by the voter. A telephone is a simple device that can be implemented in many different ways. In general, a telephone contains a speaker and microphone, along with a key pad used to input telephone numbers and possibly feature buttons such as re-dial, mute, etc.

A telephone contains a mechanism for connecting to a public communications network. However, the types of signals (analog and digital) used for transmitting information between telephones can differ. Analog telephones convert sound into analog signals that are transmitted to a receiving telephone where the signals are converted back to sound. Traditional landline telephones connect to the Public Switched Telephone Network using analog signals and communications protocols developed by the ITU-T.

Many newer types of telephones connect to the network using digital signals. Digital telephones covert sound into a digital signal (a series of ones and zeros) before passing it to the public communications network. The receiving telephone must convert the signal back to sound. There are many different types of digital telephones used today. Large organizations often use digital telephones in their offices which use a digital signal to connect to the same Public Switched Telephone Network as traditional analog telephones. Modern cellular phones communicate with cell sites using a digital signal. Communications protocols differ between cellular phone operators, but most use a GSM or CDMA-based protocol.

Voice over Internet Protocol (VoIP) telephones are a new type of digital telephone that connects to the Internet rather than the traditional telephone network. VoIP operators typically act as a bridge between the Internet and the telephone network. VoIP telephones are significantly more sophisticated than their digital and analog counterparts, and the communications protocols are often specific to a particular implementation. Many cable television operators offer VoIP telephones to their customers. The VoIP components are typically in the customer's cable modem, which connects to a traditional analog telephone. Other services allow individuals to run telephone application software (such as Skype) on general purpose computers, allowing those individuals to make and receive calls when their computers are connected to the Internet.

PUBLIC COMMUNICATION NETWORK:

The public communication network is used to connect the voting stations at a polling location to the VBP receiving station at the Central Election Office. The technology used to connect the voting stations, VBP receiving station, and the public communication network can be quite different. From a physical perspective, the connections from the voting stations, VBP receiving station, and the public communication network can be wired or wireless.

A public communication network is most often a network of networks. For example, cell phones, traditional analog telephones and VoIP phones each run on their own networks. Those networks are connected to one another, creating a much larger public communication network. Different parts of the public communication network may use different kinds of signals or communications protocols. Communications equipment (PBX, switches, etc.) is used by the network to route information to its destination and converts it as necessary. For instance, calls from a traditional analog telephone must be converted from an analog to a digital signal once they reach the telephone network backbone. Similarly, calls from a digital cell phone using the GSM protocol must be converted to the G.703 protocol if they reach the traditional telephone network.

It is difficult to determine the specific path information will take from a sender to a receiver and the conversions it will undergo along that path. Given the complex set of equipment and the uncertainty of how it will be used for a particular call, the public communication network is represented as a cloud in Figure 6.

VBP RECEIVING STATION:

The VBP receiving station is located in the Central Election Office. The VBP receiving station consists of a Central VBP Server and optionally a paper record creation device. The Central VBP Server is used to query voters for their choices and store their selections through an interactive session. The Central VBP Server is a computer that is directly connected to the public communication network via a modem bank or some other network interface. When an optional paper record creation device is part of the VBP receiving station, the paper record creation device is connected to the Central VBP Server.

ELECTION MANAGEMENT SYSTEM:

The Election Management System (EMS) is located in the Central Election Office. The EMS is used to configure the Central VBP Sever component of the VBP receiving station. In addition, the EMS can be used to consolidate election results and provide election reports. The connection between the EMS and Central VBP Server is a private communication network within the Central Election Office. The private communications network with the Central Election Office can be realized using local area network (LAN) as well as moving information on physical media (CD, flash drive, etc.) between the devices.

VERMONT'S VBP IMPLEMENTATION ARCHITECTURE

This section describes one specific VBP architecture and implementation tested by the state of Vermont to provide a more concrete example of how a VBP system can be implemented. This implementation follows the basic VBP architecture provided in Figure 6, but also has some implementation-specific characteristics.

In the polling location, telephones were used for voting (i.e. Vote Station). There was no support for voting from home or other unauthorized locations. The Central VBP Receiving Station authenticated the origin of the calls it received by checking the caller-ID (telephone number) of the telephone and a password entered by a poll worker.

The Public Communication Network used by this implementation was normal telephone land-lines. Cell phones and VOIP were not allowed except as backup for land-lines failure. To support this backup capability, the Central VBP Server has support for dynamic authorization of caller-IDs.

After the call to the Central VBP Receiving Station was authenticated (caller-ID and poll worker provided password), the poll worker entered a code to initiate the correct ballot for the voter who was about to vote, before handing the phone to the voter. The Central VBP Receiving Server then engaged in an automated dialogue in which audio prompts were sent to the voter and the voter responded by touching the appropriate keys on the keypad. For example, the basic command set might be 2 and 8 for previous/next race, 4 and 6 for previous/next candidate, and 5 for "choose this one".

After a voter completed making choices, the voter was given an audio review of the ballot (the electronic record) and then confirmed (or disconfirmed) her vote. The voter was then told to wait while the VBP Receiving Station (specifically the paper record creation component) printed out a paper ballot (with barcode and a unique but untraceable ID number) that corresponds to the ballot choices just entered. As the paper ballot was printed, the barcode (containing the voter's choices) was scanned and read back to the voter, who had to choose whether to confirm these choices or spoil the ballot. Regardless if the ballot was cast or spoiled, the paper ballot was deposited in the ballot box. When the voter spoils her ballot, an additional "spoiled ballot" document with the same ID number is also put in the box. The final count is adjusted by using the spoilers to offset the completed ballots.

The unique ID numbers on the ballot can also be used to track provisional ballots.

ISSUES WITH VBP AND THE VVSG-NI

In general, the class definition of a VBP system would have to be created and all requirements reviewed for applicability. This section looks at requirements that potentially conflict with VBP systems and provides a preliminary analysis of how those requirements would have to be modified to allow VBP.

ISSUES WITH VBP USED AS AN ACCESSIBLE VOTING SYSTEM

An interpretation of the Help America Vote Act (HAVA), reflected in the VVSG-NI's requirements, essentially requires the Acc-VS (Accessible Voting System) to accommodate all applicable disabilities, e.g., blindness, low vision, poor dexterity, and lack of mobility. Is the VBP an Acc-VS, then? For the implementation of VBP being used in Vermont, the VBP meets only some of the requirements for the Acc-VS as specified in the VVSG-NI. For example, the requirements for synchronized audio and visual and for non-manual input capability are not met. Note that those with dexterity disabilities would probably want to use a visual interface. If local officials were to deploy VBP for the blind (and for sighted voters), they would still have to accommodate other disabilities at all polling places.

There are several options that the EAC could consider:

a. Write requirements for VBP with additional capabilities to address all the accessibility requirements. The pros of this approach include that no reinterpretation of HAVA would be needed, and all voters regardless of disability could use the VBP system. The cons of this approach include that building such a system

would be costly and would seem to defeat one of the purposes of the VBP: to provide a relatively inexpensive solution for voters who are blind or who wish to use a VBP system.

b. Loosen the interpretation of conformance to allow solutions addressing different disabilities to be certified and provide guidance as to how a polling location would provide the entire capability for Acc-VS. This is an EAC policy decision. The pros of this approach include that VBP could retain its simpler focus on providing accessibility for blind voters, and this would be significantly less costly than reworking the VBP to provide accessibility for all disabilities. The cons of this approach include that polling sites would need to provide multiple devices for multiple disabilities, and that other devices designed to handle disabilities such as low vision would likely handle blindness already.

ISSUES WITH VBP USED FOR GENERAL VOTING

An audio-only system, such as a VBP, is not suitable for those who are deaf and require a visual interface, therefore each polling place would require a voting system that provides a visual interface. Our research also shows that an audio-only system is more difficult for most voters (including those who are blind) to use because listening carefully interferes with the process of voting. This may create usability problems for sighted voters, especially those with cognitive disabilities, causing more errors. Therefore, research measuring the usability of the VBP interface would be needed to determine whether an audio VBP can be designed with a lower "cognitive load" that would increase the usability.

The VVSG-NI security requirements were developed under the assumption that the voting devices would be used in physical polling places where voters would go to cast their ballots and election officials would monitor voting system equipment; the VVSG-NI security requirements were not intended to facilitate remote voting (i.e. voting not at the physical polling place). As a result, voting devices are prohibited from using public communication networks during an election to communicate with other devices located outside a polling place. As shown in Figure 6, a public communication network is generally used in a VBP system. In order to support VBP systems in the VVSG-NI, this requirement would have to be modified to allow use of public communication networks during an election to communicate outside a polling place.

The VVSG-NI includes additional requirements on communications that would be applicable to VBP systems and that may be difficult for commercially available telephones to meet. For instance, VBP telephones may be required to disable the interface used to connect to the public communication network when not in the voting state. A secure communication channel between the telephone and the Central VBP Server may be required, using cryptographic techniques such as digital signatures or message authentication codes (MAC). Furthermore, the VVSG-NI communication security requirements were not intended to protect official voter selection information in transit over a network; additional security requirements may be needed to protect this information. The communication security requirements would have to be reevaluated to determine their applicability, suitability and comprehensiveness for VBP systems.

The VVSG-NI requires voting systems to be software independent (SI). Software Independence in the VVSG-NI is accomplished through the use of Independent Voter Verifiable Records (IVVR). In general, VBP systems cannot meet the VVSG-NI requirements for Independent Voter Verifiable Records. In order to support VBP systems in the

VVSG-NI, the concept of software independence would have to be redefined somewhat. In addition, the requirements found in Part 1, Chapter 4, Security and Audit Architecture would have to be updated based on the new definition of software independence.

The VVSG-NI has software management requirements that would be difficult to meet when programmable telephones are used by a VBP system. The requirements would apply to programmable telephones that use software, firmware, or hardwired logic. Although the requirements can be met by the Central VBP Server and EMS, it may not be possible to meet these requirements using programmable telephones that are commercially available. The applicability of the software management requirements to programmable telephones would have to be resolved either by saying they do not apply or modifying the requirements.

The VVSG-NI has access control requirements that would be difficult to meet when programmable phones are used by a VBP system. The applicability of the access control requirements to programmable telephones would have to be resolved either by saying they do not apply or modifying the requirements.

CONCLUSIONS

In conclusion, accommodating VBP in the VVSG-NI as it is used in Vermont may not be possible due to interpretations made of HAVA requirements for accessibility. VBP as currently designed are also not suitable for the general voting station due to the lack of a visual interface. From a security perspective, two fundamental issues stand in the way of VBP systems being supported by the VVSG-NI: (1) allowing communication outside the polling place by a public communications networks during an election and (2) refining the concept of software independence in such as way as to allow for VBP systems.

If these fundamental issues can be addressed, there are still VVSG-NI requirements with issues that need to be resolved:

- A voting system class would need to be defined for VBP systems;
- Requirements found in Part 1, Chapter 4, Security and Audit Architecture would have to be updated based on the new definition of software independence;
- The applicability of the software management requirements to programmable telephones would need to be clarified;
- The applicability of the access control requirements to programmable telephones would need to be clarified.

Finally, there are VVSG-NI requirements that would make it difficult for VBP systems to use inexpensive commercially available products. An example is the secure communications requirements that rely on the use of cryptography, which mean essentially that the Central VBP Server and telephones would need cryptographic capabilities. Implementing cryptography in the Central VBP Server may not be difficult; implementing cryptography in telephones can be done but commercially available products are quite expensive (on the order of hundreds of dollars). Relaxing the cryptography requirements would remove one of the strongest security protections for remote communications.

VBP may be considered as a form of remote voting and thus “different enough” to warrant not intermingling VBP requirements with the requirements for precinct-based equipment in the VVSG-NI. Otherwise, the requirements for precinct-based equipment would have to be modified or weakened substantially to accommodate VBP. A preferred alternative would be to place requirements for VBP in a separate voting standard or perhaps in a special appendix of the VVSG-NI for remote voting equipment.

AREA 4: DEVELOPING A FEASIBILITY STUDY OF THE RAMIFICATIONS OF THE EAC SEPARATELY TESTING AND CERTIFYING COMPONENTS OF A VOTING SYSTEM, AND REQUIREMENTS FOR INTEROPERABILITY BETWEEN SYSTEMS AND SYSTEM COMPONENTS

Wording from the EAC: "Developing a feasibility study of the ramifications of the EAC separately testing and certifying components of a voting system, and requirements for interoperability between systems and system components. In addressing this, the EAC would ask NIST to address the feasibility of requiring, in the VVSG-NI, a specific standard for the format of electronic election data and the inclusion of requirements for standard methods for exporting electronic election data."

SUMMARY

There are four separate questions in this request, as follows:

1. What are the ramifications of separately testing and certifying voting devices?
2. What would a requirement for interoperability look like?
3. What is the feasibility of requiring, in the VVSG-NI, a specific standard for the format of electronic election data?
4. What is the feasibility of requiring, in the VVSG-NI, standard methods for exporting electronic election data?

It is possible to separately test and certify voting devices; however, this would represent a significant change in philosophy from the current VVSG-NI and current EAC and test lab procedures. The pros of doing this might include the potential for cheaper and more flexible voting systems that could be composed of off-the-shelf products designed to be interchangeable. The cons would include that the architecture and interfaces, protocols, and data formats would need to be precisely specified and an interoperability testing program would need to be created. Defining these items could be restrictive to manufacturers and require hardware design changes. At the end, the voting system would still need to be tested as a complete unit.

A requirement for interoperability would need to define explicitly what exactly must interoperate with what and how the interoperability is to be achieved. The VVSG-NI conformance testing does not address interoperability, and while conformance to a standard is advisable for interoperability, it does not guarantee it. Thus, a separate interoperability testing program would need to be created.

A standardized format for election data could be specified in the VVSG-NI provided it supports all voting variations, has a coherent data model with strong conceptual integrity such that interoperability among manufacturers is possible, and has been vetted by the manufacturers. The pros of doing this include most significantly that every vendor would be required to use this format and interoperability of data from different devices and manufacturers would be encouraged. The cons of doing this include that, currently, no specific standard in existence meets

essential requirements of supporting all VVSG-NI voting variations, of having been vetted by U.S. voting system manufacturers, of being simple and unambiguous to implement, and of demonstrated interoperability. The VVSG-NI currently specifies that voting systems must use a standardized format, but not a specific standard.

Lastly, there is another prerequisite for interoperability: a way to get the data *out*. For standards-based interoperability, one needs not only a standard interchange format but also standard methods for exporting the data. Otherwise, the data could be impossible to export, making the exchange format moot. But such an export method would impose a design requirement that might quickly be overtaken by technological improvements. The approach currently taken in the VVSG-NI of specifying that the data must be in *some* standardized format and that it must be exportable *somehow* may ultimately be preferable.

The following sections go into these questions in more detail.

RAMIFICATIONS OF DEVICE LEVEL TESTING AND CERTIFICATION

The VVSG-NI assumes that voting systems will be tested as a whole; there is no concept of device level certification. Permitting this would be a significant change in philosophy, which would affect many aspects of the VVSG-NI and, likely, many EAC and test lab procedures and processes. The following sections and go into more detail about the issues involved in device level testing and certification.

PRESCRIBED ARCHITECTURE

In order for certification of a device to have any practical meaning, it is necessary to have some idea of how that device integrates with others and what its functions and responsibilities within the voting system are. In other words, we need to know the architecture of the voting system.

The VVSG-NI does not specify an architectural model. Manufacturers are currently free to invent new ways of satisfying the requirements of the voting process using new kinds and combinations of devices. It would be feasible to add an architectural model for voting systems to the VVSG-NI, but there are two major drawbacks to doing so:

1. Developing a standard architectural model would take considerable time and resources, and
2. A specific architectural model would limit innovation.

NO ASSURANCE OF SYSTEM-LEVEL CONFORMANCE

Another question to consider is, how does one ensure that an integrated system—that is, a system composed of devices that have been separately tested and certified—works correctly and conforms to the VVSG-NI? To state that a voting system is conformant to the VVSG-NI requires the entire system to be tested.

Voting system conformance has many dimensions—accessibility, usability, privacy, secrecy, auditability, etc.—and most of these dimensions do not have anything analogous to a fault tree analysis that one can perform. Some high-level properties are holistic and have no logical connection to low-level properties at all. Thus we conclude that a valid, general model relating voting system conformance to the conformance of its constituent devices is probably infeasible even if an architecture were prescribed.

A REQUIREMENT FOR INTEROPERABILITY

A requirement saying simply *voting devices shall be interoperable* would be well-intentioned but not especially useful. Interoperability is an attribute not of a device, but of the relationship between two or more devices. One cannot meaningfully say that a device is interoperable without answering the question *with what*?

In practice, the intent of the above requirement must be separated into two synergistic concerns: conformance to data format and interface standards, and demonstrated interoperability with one or more products from other manufacturers. This truth and its consequences are explored in more detail in the following subsections.

RELEVANCE OF STANDARDS TO INTEROPERABILITY

Conformance to a standard is a necessary but not necessarily sufficient means to achieve interoperability. Depending on the composition of the system under test, it can be insufficient because it is generally possible to construct an integration scenario in which a failure will occur because of some property that was not explicitly modeled in the standard.

The value of conformance to data format and interface standards is not in providing a guarantee of interoperability for devices that have never before been integrated, but in reducing the cost of performing that integration. Greater commonality in the data elements and interfaces implemented by the devices usually means a lower integration cost. In the best possible case, it could, in theory, be zero (i.e., works first time).

However, even with conformance to the same data format and interface, a successful integration is by no means assured; a wide variety of technical, semantic, functional, policy, and logistical conflicts can arise when integration is attempted.

INTEROPERABILITY TESTING

Since interoperability is an attribute of the relationship between two or more devices, conformance testing of a device by itself reveals little about interoperability. Instead, interoperability testing must be conducted with all of the devices that are intended to work together. Interoperability testing consists of bringing together existing products, configuring them to work together, and performing an operational test to determine whether they are in fact capable of working together.

Manufacturers of products that implement networking and data communications protocols have historically achieved and maintained interoperability through voluntary, manufacturer-driven interoperability testing events known as *plugfests*. Manufacturers get their products to work with the products of whichever other manufacturers show up for the plugfest. Plugfests are held periodically to ensure that interoperability is maintained as products evolve and new products appear. The University of New Hampshire's InterOperability Laboratory currently hosts plugfests for implementers of many different networking and data communications protocols.

If interoperability testing were to be driven by mandate rather than voluntary manufacturer commitment, the authority issuing the mandate (i.e., the EAC) would be obliged either to choose the specific products with which interoperability must be demonstrated (unavoidably granting a competitive advantage to those products) or to define a process through which that choice would be made. The corresponding VVSG-NI product requirements would then be of the form either

> Voting devices shall interoperate with X, Y and Z,

or

> Voting devices shall interoperate with the pool of reference implementations determined by process P,

and interoperability testing would be specified as the test method. There would need to be a collection of such requirements to mandate interoperability across each interface in the standard architecture.

FEASIBILITY OF STANDARD DATA FORMAT IN THE VVSG-NI

Currently, the VVSG-NI specifies use of a standardized data format, but does not require a specific format to use. This does contain some advantages in that it allows manufacturers to determine the format they wish to use, and translators could be provided to make the data interchangeable with that of other formats. If a data format were to be mandated by the VVSG-NI, it should meet the following conditions:

1. It should support all of the voting variations defined in the VVSG-NI;
2. It should have a coherent data model with strong conceptual integrity;
3. It should be vetted by U.S. voting system manufacturers to ensure that it contains no critical errors or omissions; and
4. In the spirit of HAVA §221 (42 U.S.C. 15361) (e)(3), it should be unencumbered by any copyrights, patents, or trade secrets that would oblige VVSG-NI implementers to pay royalties to or sign agreements with intellectual property owners.

Unfortunately, NIST is unaware of any existing candidate standard that satisfies or is near to satisfying those conditions. To specify a standard data format in the VVSG-NI, it would be necessary either to compromise on the above conditions or to make VVSG-NI finalization dependent on the successful completion of a lengthy process of standards development and/or revision.

ELECTION MARKUP LANGUAGE (EML)

Election Markup Language (EML) is often cited as the only viable standard for election data exchange. However, previous NIST analysis found that some voting variations for US elections either were not handled or could be handled only by changing or working around standard EML definitions. EML schemas allow for different interpretations and extensions, but reinterpreting and changing the standard defeats the goal of standards-based interoperability (it becomes just another ad hoc integration). Although some demonstrations have been performed, implementation experience with EML remains limited.

IEEE P1622

Institute of Electrical and Electronics Engineers (IEEE) Project 1622, Voting Systems Electronic Data Interchange was chartered to develop electronic data interchange formats for use by voting devices. It produced a draft standard in which concepts from an unpublished schema developed by the Open Voting Consortium (OVC) were mapped into EML and EDX (see below). The draft standard remains unpublished and unavailable to the general public.

EDX (acronym expansion unknown) is a specification that Hart InterCivic promulgated as a candidate for standardization. Hart indicated informally that it would waive its copyright over EDX if EDX were adopted as part of IEEE P1622. Failing that, EDX remains the intellectual property of Hart InterCivic.

The P1622 draft went to ballot in March 2007, but the balloting process was aborted to make way for a reorganization of the parent committee (Standards Coordinating Committee 38). There has been no activity in P1622 since then (as of 2008-03-07). The parent committee has not yet completed revisions to its policies and procedures, but there has been activity there. Thus, while Project 1622 remains officially alive, it has been in limbo for a year, and is difficult to project the likelihood or time frame in which IEEE might approve a P1622 standard.

Since the P1622 draft does not specify an independent data format, the most significant impact of its approval would be for EDX possibly to become available and usable as an alternative to EML. However, unless some special arrangement were made, users would need to purchase a copy of the P1622 standard to obtain access to the EDX schema. IEEE normally asserts full copyright over its standards and prohibits free copying.

OTHER

Various projects in academia and even at NIST have developed data models that could serve as the basis for an election data format standard. However, the process of evolving such a model into a credible data format standard and then vetting that standard with manufacturers and other stakeholders would essentially be yet another standardization effort facing the same hazards as previous attempts. Given sufficient time, resources, and political capital, it is possible that a standard tailored to the goals of the EAC could be developed, but it is unlikely

that consensus for another standard could be built in a time scale that would fit within the planned release of the VVSG-NI. Prior commitments to EML or proprietary data formats might prevent any public support for another standard from emerging.

FEASIBILITY OF STANDARD DATA EXPORT METHOD IN THE VVSG-NI

Mandating a data export method is relatively uncomplicated. However, as discussed already, conformance to an interface standard in and of itself is insufficient to yield interoperability, and it does not necessarily empower end users to achieve their integration goals.

Like many design requirements, a mandatory data export method would live on borrowed time with respect to the regular and rapid "churn" of information technology. There is a significant risk that the equipment or software necessary to use the mandated interface might become obsolete before the VVSG-NI is finalized, and quite high probability that it would do so before the anticipated retirement of voting systems certified to the VVSG-NI.

AREA 5: PRODUCING A STUDY ON THE IMPACT OF THE THE VVSG-NI ON EARLY VOTING OR VOTE CENTERS.

Wording from the EAC*:* "Producing a study on the impact of the next iteration of the VVSG on early voting or vote centers. This research should address questions that have been raised as to whether existing requirements in the next iteration of the VVSG, as written, would prohibit or impact the use of voting equipment in early voting or in vote centers. This is especially of concern with regard to the use of electronic pollbooks."

SUMMARY AND CONCLUSIONS

During the writing of the VVSG-NI, NIST and the TGDC anticipated the use of voting systems for early voting and in (multi-precinct) vote centers. Early voting is handled through the distinction between open polls-close polls and suspend-resume voting that is explained in Part 1 Section 8.2; thus, there appear to be no issues with accommodating early voting in the VVSG-NI.

The VVPAT requirements were updated to accommodate use in multi-precinct vote centers, specifically to individually label each paper cast vote record (CVR) on a paper spool with an identification of the corresponding precinct. This facilitates auditing when a VVPAT voting system is used in multi-precinct vote centers and the same paper roll contains CVRs from multiple precincts; without the precinct identification on each CVR, it would be difficult to determine which CVRs "belong" to which precinct.

Otherwise in the VVSG-NI, the only conflict for vote centers appears to be in the definition of precinct, which maintains the historical assumption that a precinct is associated with a specific polling place. It should be possible to relieve that conflict with a minor tweak of the definition (e.g., "...typically cast ballots at the same polling place, unless an alternative such as vote centers or absentee voting is used").

An electronic poll book is essentially a laptop computer containing a voter registration database; its purpose is to assist in automating the operations of checking voters in at the polls and in some cases enabling the appropriate ballot. There appear to be no requirements or issues with regard to the VVSG-NI that would prevent electronic pollbooks from being used in early voting or in vote centers.

AREA 6: GOAL LEVEL REQUIREMENTS

Wording from the EAC: "Identifying all so-called "goal level requirements" in the TGDC draft recommendations and developing alternatives to the inclusion of this information in the body of the VVSG-NI."

SUMMARY

A goal level requirement (herein referred to as a "goal requirement") is, in general, a requirement that purposely may be broad and less precise as opposed to being very specific. It states and requires a desired performance or behavior, but does not specifically state how that performance or behavior is to be met or to what level it is to be achieved. As a consequence, the question of whether the goal has been satisfied may be difficult to ascertain; it may be difficult to test or to imagine a test that would precisely answer the question of whether the requirement has been met. Goal requirements are not necessarily good or bad; they are used for specific purposes.

The pros of using goal requirements in this way include:

- The requirement can be used to clearly state the intent or desired performance;
- It avoids constraining design when constraining designs is not desired or is premature;
- It does not necessarily constrain the amount of testing needed to test conformance to the requirement.

The cons of using goal requirements include:

- The pass/fail criteria may be unclear to vendors and test labs;
- The tests may be subjective and difficult to make uniform across multiple labs.

The VVSG-NI contains a relatively small number, less than 20, of goal requirements. There are some requirements in the VVSG-NI that may appear to be goal requirements but that can, in fact, be tested consistently using "expert analysis" or "expert review", that is, using an expert or qualified specialist in a particular field to determine whether the requirement has been met. Other goal requirements can be made into more specific design level requirements; however, doing so at this point may unwisely constrain designs.

HOW ARE GOAL REQUIREMENTS USED IN THE VVSG-NI?

The VVSG-NI uses goal requirements in two ways. First and most commonly, goal requirements are used as a top-level requirement in combination with sub-requirements; the top-level goal requirement is made more specific and testable by the resultant sub-requirements. The primary reason for doing this is to aid understandability of the requirement by clearly stating the goal (the desired behavior) up-front in the requirement. It binds together

the sub-requirements that follow and serves also to make them more understandable. NIST does not consider that the identification of these sorts of goal requirements is intended by this task.

A second rationale for using goal requirements is when a particular type of performance is desired or needs to be encouraged, but it cannot be or is not, for various reasons, explicitly specified. The reasons for doing this generally are:

- It may be premature to specify the requirement in more specific terms, i.e., a specific technology around the requirement may not yet be well-developed and specifying it now might overly constrain vendor designs, and
- It may be expensive or time-consuming or premature to make the requirement objectively testable, e.g., developing performance benchmarks.

This type of goal requirement represents a trade-off in that it may be the best choice in a given situation; the alternatives would otherwise be to not include the requirement at all or take action to make the requirement more objectively testable, which, as noted, could do more harm than good.

GOAL-LIKE REQUIREMENTS REQUIRING EXPERT ANALYSIS

There are some requirements in the VVSG-NI that may appear to be goal requirements but that can, in fact, be tested consistently using "expert analysis," sometimes called "expert review," that is, using an expert or qualified specialist in a particular field to determine whether the requirement has been met. For example, consider Requirement part1:3.2.8.1-A *Ease of normal operation*:

> **THE PROCEDURES FOR SYSTEM SETUP, POLLING, AND SHUTDOWN, AS DOCUMENTED BY THE MANUFACTURER, SHALL BE REASONABLY EASY FOR THE TYPICAL POLL WORKER TO LEARN, UNDERSTAND, AND PERFORM.**

A usability expert with appropriate knowledge of typical poll worker characteristics and poll worker procedures along with observation of a small number of tests with typical pollworkers can determine whether the procedures in question are reasonably easy. An incorrect or missing important instruction in the documentation or great difficulty due to poor design will be readily observable and a set of experts would agree. (While the requirement conceivably could be rewritten to be more specific about what, exactly, constitutes easy, it may not necessarily be possible to get away completely from requiring some level of expert analysis testing.)

Contrast this with Requirement part1:6.6-A *Integratability of systems and devices*:

> **SYSTEMS SHALL MAXIMIZE INTEGRATABILITY WITH OTHER SYSTEMS AND/OR DEVICES OF OTHER SYSTEMS.**

This requirement cannot be tested consistently with expert analysis, as the question being asked by the requirement, i.e., is the system integratable enough?, is not specific about what must integrate with what for what purpose. Thus, experts could readily differ with each other over the answer, and one's own biases may become too great a factor in the decision.

A relatively small number of requirements in the VVSG-NI are written specifically with expert analysis in mind. For example, some requirements in the Human Factors Chapter 3 of Part 1 rely on expert analysis and use words such as "SHALL be reasonably easy," "SHALL be presented at a level appropriate," or "SHALL enable the poll worker to verify." Accordingly, these requirements are not included in this task.

HFP GOAL REQUIREMENTS

REQUIREMENT PART1:3.2.3.1-A SYSTEM SUPPORT OF PRIVACY

THE VOTING SYSTEM SHALL PREVENT OTHERS FROM DETERMINING THE CONTENTS OF A BALLOT.

Why goal: This requirement's goal is that it be impossible to link a cast ballot with a specific voter, assuming that the ballot has been cast directly by a voter at a voting station. This would seem not to apply to absentee voting. This requirement is a high-level goal of voting systems in general, and it includes several specific sub-requirements that relate to privacy for the voter while voting. However, there are no requirements that deal specifically with privacy of ballots after they are cast or privacy of information about the voter prior to casting, although there are some requirements relating to privacy and electronic pollbooks in other sections of the VVSG-NI. As written, testing this requirement may place too much emphasis on expert analysis.

Options:

1. Create a larger section in the VVSG-NI for privacy requirements and ensure all requirements dealing with privacy and other sections of the VVSG-NI are placed in the privacy section or are cross-referenced accordingly.

2. In addition to option 2, research further requirements for privacy that are testable.

REQUIREMENT PART1:3.3.7-A GENERAL SUPPORT FOR COGNITIVE DISABILITIES

THE ACCESSIBLE VOTING STATION SHOULD PROVIDE SUPPORT TO VOTERS WITH COGNITIVE DISABILITIES.

Why goal: This requirement's goal is that the voting system as a whole provides sufficient support to voters with cognitive disabilities so that they are able to vote independently. However, what constitutes a cognitive disability and how it should be accommodated is not clear; handling this particular disability in the VVSG-NI is much less clear than handling disabilities for, say, blindness or partial vision.

There are other usability and accessibility requirements that support cognitive disabilities, such as plain language and synchronized audio and video. But beyond that, the VVSG-NI does not contain requirements for providing support to voters with cognitive disabilities.

Options:

1. Keep the requirement as-is and establish minimal expert analysis criteria that would be included as part of the test suite being written by NIST. *NOTE: this is the approach being taken by NIST as it is writing the HFP test suite.*

2. Conduct longer-term research on cognitive disabilities and create specific, testable requirements.

STS GOAL REQUIREMENTS

3.1 – REQUIREMENT PART1:4.2.1-A VOTING SYSTEM, SUPPORT FOR POLLBOOK AUDIT

THE VOTING SYSTEM SHALL SUPPORT A SECURE POLLBOOK AUDIT THAT CAN DETECT DIFFERENCES IN BALLOT COUNTS BETWEEN THE POLLBOOKS, VOTE-CAPTURE DEVICES, ACTIVATION DEVICES, AND TABULATORS.

Why goal: This requirement's goal is that the voting system as a whole produce records that are sufficient to determine if the ballot count is accurate. It more or less says that there should be traceability of the ballot count throughout all the mentioned devices back to the pollbook (or electronic pollbook). According to the Discussion field of the requirement, there is also intent that the traceability be readily usable to election officials.

But, the use of the word "secure" is problematic and the requirement does not itself contain any mention of usability. It would probably be difficult for expert analysis to consistently test this requirement across test labs.

Options:

1. Keep the requirement as-is and establish minimal expert analysis criteria that would be included as part of the test suite being written by NIST.

2. Rewrite the requirement as one or more auditing performance-based requirements that would, in essence, require full traceability of ballot counts throughout the voting system.

3. In addition to option 2, establish usability criteria for the audit and rewrite the requirement accordingly. This would require that NIST perform research with usability and security experts and election officials. This would require an approximate timeframe of 1 year and .5 million dollars.

3.2 - REQUIREMENT PART1:4.2.2-A IVVR, SUPPORT FOR HAND AUDIT

THE VOTING SYSTEM SHALL SUPPORT A HAND AUDIT OF IVVRS THAT CAN DETECT DIFFERENCES BETWEEN THE IVVR AND THE ELECTRONIC CVR.

Why goal: This requirement's aim, in part, is to ensure that the voting system produces records that are adequate and usable by election officials for conducting audits of IVVR records by hand. It thus has a usability aspect. It sets a goal for vendors to produce systems whose records, both electronic and IVVR, are easily compared. Testing the

usability aspect would require expert analysis at a minimum, as there is no performance benchmark established for hand-auditability of IVVRs.

Options:

1. Keep the requirement as-is and establish minimal expert analysis criteria for the usability of the records that would be included as part of the test suite being written by NIST.

2. Rewrite the requirement as one or more auditing performance-based requirements that would, in essence, require full traceability of ballot counts throughout the voting system.

3. In addition to option 2, establish design criteria for the IVVR such as size, durability, font sizes, layout of data, etc., and rewrite the requirement accordingly. Establishing design criteria would require further research with election officials, vendors, and usability experts, with an approximate timeframe of one year.

4. In addition to option 2, establish a performance benchmark and rewrite the requirement accordingly. To establish the performance benchmark, NIST would likely undertake a research effort similar to that used to establish performance benchmarks for voting system interfaces for voters. Such an effort would need to focus on postelection processes and how electronic and paper records are used, and then establish benchmarks for the postelection audits that are, at a minimum, needed to ensure that an election is software independent. This would require an approximate timeframe of one to three years and require funding similar to that used for the previous performance benchmark research—approximately 1-2 million dollars.

3.3 – REQUIREMENT PART1:4.2.3-A EMS, SUPPORT FOR RECONCILING VOTING DEVICE TOTALS

THE EMS SHALL SUPPORT THE RECONCILIATION OF THE TABULATOR TOTALS AND THE FINAL BALLOT COUNT AND VOTE TOTALS ACCORDING TO THE FOLLOWING:

1. **A TABULATOR WHOSE REPORTED TOTALS ARE NOT CORRECTLY INCLUDED IN THE BALLOT COUNT AND VOTE TOTAL REPORTS, AND WHICH IS AUDITED, SHALL BE DETECTABLE;**
2. **A DIFFERENCE BETWEEN THE FINAL BALLOT COUNT AND VOTE TOTALS AND THE AUDIT RECORDS FOR A TABULATOR THAT IS AUDITED SHALL BE DETECTABLE;**
3. **THE DISAGREEMENTS IN RECORDS SHALL BE DETECTABLE EVEN WHEN THE ELECTION MANAGEMENT SOFTWARE IS ACTING IN A MALICIOUS WAY; AND**
4. **THE EMS SHALL BE ABLE TO PROVIDE REPORTS THAT SUPPORT BALLOT COUNT AND VOTE TOTAL AUDITING FOR DIFFERENT REPORTING CONTEXTS.**

Why goal: This requirement's aim, in part, is to ensure that the EMS shall be able to detect errors in ballot counts and tabulator totals—that all the votes add up properly. It is similar to requirement part1:4.2.1-A in that it demands traceability of the ballot counts and totals back to the tabulator.

However, in (3), it does not specify what constitutes "acting in a malicious way." It would likely be difficult for expert analysis to consistently test this requirement across test labs.

Options:

1. Keep the requirement as-is and establish minimal expert analysis criteria for what constitutes “acting in a malicious way” that would be included as part of the test suite being written by NIST.

2. Rewrite the requirement as one or more auditing performance-based requirements that would, in essence, require full traceability of ballot counts and vote counts throughout the voting system. The auditing performance requirements would demand that *any* error be traceable and detectable; this would eliminate the “malicious” aspect of this requirement.

3.4 – REQUIREMENT PART 3:5.4.3-C RULES OF ENGAGEMENT – ADEQUATE THREAT MODEL

THE OEVT TEAM SHALL VERIFY THAT THE THREAT MODEL SUFFICIENTLY ADDRESSES SIGNIFICANT THREATS TO THE VOTING SYSTEM.

Why goal: This requirement specifies that the OEVT team shall inspect the threat model supplied by the vendor and determine whether it sufficiently addresses significant threats to the voting system.

However, there is no a priori specification of significant threats to the voting system; thus, it is left to the OEVT team to decide what is significant and so forth. Different experts in voting system vulnerabilities may disagree as to the composition of the threat model, but this is greatly compounded when different testing labs are involved and have to make a determination whether the threat model sufficiently addresses what they deem to be significant threats.

If there is not some up-front determination of significant threats that all testing labs agreed to, it would likely be difficult for expert analysis to consistently test this requirement across test labs.

Options:

1. Keep the requirement as-is and establish minimal expert analysis criteria for what constitutes "significant threats to the voting system."

2. Use a threat model to be generated by the EAC’s risk assessment contract.

3. If the EAC undertakes a voting systems risk assessment, use the threat model that will result from the risk assessment.

CRT GOAL REQUIREMENTS

REQUIREMENT PART1:6.4.1.3-A ACCEPTABLE CODING CONVENTIONS

APPLICATION LOGIC SHALL ADHERE TO A PUBLISHED, CREDIBLE SET OF CODING RULES, CONVENTIONS OR STANDARDS (HEREIN SIMPLY CALLED "CODING CONVENTIONS") THAT ENHANCE THE WORKMANSHIP, SECURITY, INTEGRITY, TESTABILITY, AND MAINTAINABILITY OF APPLICATIONS.

Why goal: This requirement's sub-requirements define "published" and "credible" in testable terms, but the intent is stated to help prevent loopholes and resolve any disputes that may arise about what sort of coding conventions are acceptable. The statement of the intent makes it easier for the certifying authority to prevent such loopholes from being exploited successfully.

Options:

1. Keep the requirement as-is and apply expert analysis to supplement the definitions of "published" and "credible" that appear in the subrequirements.

2. Specify concrete coding conventions to be used. A con of this approach is that the VSS 2002 specified concrete coding conventions, but they were obsolete almost immediately.

REQUIREMENT PART1:6.4.1.4-B MODULE SIZE AND IDENTIFICATION

MODULES SHALL BE SMALL AND EASILY IDENTIFIABLE.

Why goal: This requirement's sub-requirements specify maximum module size in testable terms, but they are SHOULDs because they can't be applied universally.

Options:

1. Keep the requirement as-is and apply expert analysis as to what is a small and easily identifiable module, using the SHOULDs in subrequirements as guidance.

2. In public comments, iBeta has suggested replacing the lines-of-code metric (which was carried over from 2002/2005) with cyclomatic complexity. If the SHOULD sub-requirements are changed to a SHALL requirement based on cyclomatic complexity, this requirement could be deleted.

REQUIREMENT PART 1:6.6-A INTEGRATABILITY OF SYSTEMS AND DEVICES

SYSTEMS SHALL MAXIMIZE INTEGRATABILITY WITH OTHER SYSTEMS AND/OR DEVICES OF OTHER SYSTEMS.

Why goal: This requirement has a goal of promoting interoperability of voting system devices among and across manufacturers. The intent is that vendors architect voting systems so that they can, where possible, consist of components that can interoperate with other, similar components possibly produced by different vendors.

This is a laudable goal, but without specifying exactly what must integrate with what for what purpose, testing whether a vendor has satisfied this requirement or not is virtually impossible. As such, this requirement states a goal but is untestable.

Options:

1. Keep the requirement as-is and update the requirement when more information is known about voting system components and interfaces.

2. Define a standard architecture and create the design requirements around it. For example, the "accessibility" roundtable discussion at Gallaudet University brought out that people may wish to bring their own accessibility devices to the polling place, which would indicate that this is one area where design requirements for voting system interfaces could be specified. The EAC would need to also create an interoperability testing program.

3. Select a pool of "other systems and/or devices" with which integration must be demonstrated in order to demonstrate conformity to the requirement, or define a process by which those other systems and/or devices are selected.