Context Description: Posted Dec. 1, 2006

This draft report was prepared by NIST staff at the request of the Technical Guidelines Development Committee (TGDC) to serve as a point of discussion at the Dec. 4-5 meeting of the TGDC. Prepared in conjunction with members of a TGDC subcommittee, the report is a discussion draft and does not represent a consensus view or recommendation from either NIST or the TGDC. It reflects the conclusions of NIST research staff for purposes of discussion. The TGDC is an advisory group to the Election Assistance Commission, which produces voluntary voting system guidelines and was established by the Help America Vote Act. NIST serves as a technical advisor to the TGDC.

The NIST research and the draft report's conclusions are based on interviews and discussions with election officials, voting system vendors, computer scientists, and other experts in the field, as well as a literature search and the technical expertise of its authors. It is intended to help in developing guidelines for the next generation of electronic voting machine to ensure that these systems are as reliable, accurate, and secure as possible. Issues of certification or decertification of voting systems currently in place are outside the scope of this document and of the TGDC's deliberations.

Requiring Software Independence in VVSG 2007: STS Recommendations for the TGDC

William Burr, John Kelsey, Rene Peralta, John Wack
National Institute of Standards and Technology
November 2006

Acronyms and Terms Used in This Paper

The following acronyms and terms are used in this paper. Some of these terms are also defined in the draft VVSG 2007 glossary, located at http://vote.nist.gov/TGDC/VVSG2007-glossary-20061011.doc.

- **ASIC** – Application-Specific Integrated Circuit, a special-purpose chip, used in voting systems
- **Ballot of Record** – the ballot used as the official record of a voter's choices in an election
- **EBM** – Electronic Ballot Marking device, e.g., the ES&S AutoMARK
- **CRT** – Core Requirements and Testing subcommittee of the TGDC
- **CVR** – Cast Vote Record

- **DRE** – Direct Record Electronic, used in this paper to refer to current "blackbox" DREs that provide no transparency to its software, e.g., open source, etc.
- **E2E** – End-to-end auditable voting systems, usually based on cryptography
- **HFP** – Human Factors and Privacy subcommittee of the TGDC
- **IDV/IV** – Independent Dual Verification, shortened to Independent Verification
- **MTBF** – Mean Time Between Failure
- **Op Scan** – voting systems in which a voter completes a paper ballot, either by hand or via an EBM, and then the ballot is scanned by an optical scanner
- **OEVT** – Open Ended Vulnerability Testing
- **PROM** – Programmable Read-Only Memory that can be programmed, used in voting systems
- **SI** – Software Independence or Independent
- **Software IV** – Independent Verification approach performed using software such that the IV record(s) are all-electronic
- **STS** - Security and Transparency Subcommittee of the TGDC
- **TGDC** - Technical Guidelines Development Committee
- **DRE-VVPAT** – A DRE with Voter Verified Paper Audit Trail voting system
- **VVPR** – Voter Verified Paper Records
- **VVSG** – Voluntary Voting Systems Guidelines

1. Introduction

The purpose of this paper is to summarize various issues and make recommendations from the STS regarding the types of voting systems that should be required in the VVSG 2007. It describes the concept of Software Independence (SI) in voting systems and how it relates to Independent (Dual) Verification (IDV or IV)[1]. The recommendations in this paper include requiring that voting systems meet the definition of SI in VVSG 2007[2].

This paper also presents conclusions regarding the feasibility of including testable requirements for paperless and cryptographic SI voting systems in VVSG 2007. It also includes discussion of a new category of voting systems, called the Innovation Class, whose purpose is to foster commercial development and subsequent certification of paperless and cryptographic approaches to SI voting systems.

1.1 The Concept of Software-Independence in Voting Systems

A voting system is software-independent if a previously undetected change or error in its software cannot cause an undetectable change or error in an election outcome. In other words, it can be positively determined whether the voting system's (typically, electronic) CVRs are accurate as cast by the voter or in error. In SI voting systems that are readily available today, the determination can be made via the use of independent audits of the electronic counts or CVRs, and independent voter-verified paper records used as the audit trail.

[1] IDV is the term used in VVSG 2005. Since then, IV has been used to mean the same thing.

[2] This paper builds on an earlier paper that introduced the concept of software-independent voting systems but that did not contain STS recommendations. This earlier paper is available at http://vote.nist.gov/SI-in-voting.pdf.

A simple example of this is op scan, in which a voter marks (by hand or using an EBM) the paper ballot. The voter verifies the paper ballot is correct, thus it is *voter-verified*, and the paper ballot is "outside" or *independent* of the voting system, i.e., it cannot be changed or modified by the voting system. As a consequence of these two factors, the paper ballot can be considered as *independent evidence* of what the voter believed he or she was casting. After the paper ballots are scanned, they can subsequently be used to provide an *independent audit*, or check, on the accuracy of the electronic counts.

If an undetected change or error in the optical scanner's software were to cause erroneous counts, subsequent audits would show the errors. Even if malicious code was inserted into the scanner's software, the audits would detect resultant errors in the counts. Therefore, the correctness of the scanner's counts does not rely on the correctness of the scanner's software, and thus op scan is software independent: changes or errors in its software will be reliably detected by independent audits of its electronic counts. Thus, the primary ingredients to SI as illustrated in op scan are (1) *voter-verified records* that are (2) *independent* of the voting system used in (3) *audits* of the scanner's electronic counts.

The approach to software-independence used in op scan is based on voter-verified paper records, but some all-electronic paperless approaches have been proposed. It is a research topic currently as to whether software independence may be able to be accomplished via systems that would produce an all-electronic voter-verified, independent audit trail (known as *software IV* systems). In cryptographic E2E voting systems, there may be no audit trail in the sense of what exists with op scan or DRE-VVPAT, but the correctness of the election results can still be proven via the cryptographic protocol that the system is based upon. E2E systems are an active research topic and one E2E approach has been marketed[3].

1.2 What is Software-Dependence?

A voting system is software-dependent if the correctness of the election results is dependent on the correctness of the software and on whatever assurances can be obtained that the software on the voting machine is in fact the software that is supposed to be there. It is, to a much greater extent, more vulnerable to undetected programming errors or malicious code.

The most obvious example of a software-dependent voting system is the DRE, which does not produce an independent voter-verified audit trail. Therefore, audits of its electronic records cannot be against any independent evidence of the voter's intentions as cast and as a consequence, its electronic records cannot be audited independently. The accuracy of the electronic records has to be ascertained in some other way, which in this case would be by trusting that its software is correct and has remained error-free. Verifying that this is the case is so complex as to be infeasible; current testing methods could not guarantee this.

2. Background and Overview

The very close 2000 presidential election highlighted problems with the accuracy and usability of then current voting systems. In 2002 Congress passed the Help America Vote Act (HAVA) creating the Election Assistance Commission (EAC), with a Technical Guideline Development Committee (TGDC), and assigned NIST to provide support for the TGDC. Congress also provided funding to buy new voting machines, to avoid a repeat of the

[3] See http://www.votehere.com.

problems with the 2000 election. Many states bought Direct Recording Electronic (DRE) machines with that money.

2.1 DRE Systems and Security

DRE machines are essentially notebook computers programmed to display ballot images, record voter choices, and store the electronic CVRs on removable memory cards. They are comparatively easy to use, particularly by those with impaired vision; they can also produce an audio ballot for blind voters. They typically produce a start-of-day zero report and an end-of-day summary printout of the ballots cast on the machine, but they do not require or produce paper ballots, and it is this aspect that has helped to make them popular with election officials who have had to deal with logistical and accuracy problems and historical fraud in handling and counting paper ballots.

But many people, especially in the computer engineering and security community, assert that DREs are vulnerable to undetectable errors as well as malicious software attacks because there is no audit mechanism other than what the DRE can report on: how many records it has stored, ballot styles, etc. Potentially, a single programmer could "rig" a major election. The computer security community rejects the notion that DREs can be made secure, arguing that their design is inadequate to meet the requirements of voting and that they are vulnerable to large-scale errors and election fraud.

2.2 State Requirements for VVPR

State legislatures have responded: 6 of the top 10 most populous states use or soon will be using voter-verified paper records throughout (CA, NY, IL, OH, MI, and NJ); in 3 of the remaining 4 states (TX, FL, PA) it varies from county to county (e.g., in Florida 52 of 67 counties use op scan plus an accessible device)[4].

A summary of state usage is as follows:

- 27 states mandate voter-verified paper records statewide
- 8 don't mandate them but use them statewide
- 10 use them on a county-by-county basis
- 5 states use only DREs statewide (DE, GA, LA, MD, SC)

Thus a total of 35 states use voter-verified paper records throughout. Over half of all voters in the 2006 elections used voter-verified paper records; 49% of voters alone used op scan [5].

2.3 NIST and STS Determinations

In its research for writing requirements for electronic voting systems, NIST has investigated a broad range of issues in electronic voting. NIST has held numerous teleconferences with the TGDC and with vendors and election officials. It has visited and inspected voting system testing laboratories. NIST has worked with experts in areas such as voting system security,

[4] See http://www.house.gov/science/hearings/full06/July%2019/Wagner.pdf and http://www.verifiedvoting.org/index.php.

[5] See http://www.edssurvey.com/images/File/ve2006_nrpt.pdf.

auditing, reliability, testing, usability, and accessibility, and has looked to other areas of IT computing for input and ideas that would be useful in a voting context (one area, gaming and state lottery systems, has many interesting overlaps with voting system issues[6]). Because NIST is primarily an engineering-based institution, it has taken pains to learn about the realities of elections. NIST voting-team staff have volunteered as poll workers and election judges, and have observed other elections and official canvassing and counting activities. NIST has researched many issues and irregularities in elections and, as opposed to relying solely on the press and published articles, has gone directly to those election officials involved.

One conclusion drawn by NIST is that the lack of an independent audit capability in DRE voting systems is one of the main reasons behind continued questions about voting system security and diminished public confidence in elections. NIST does not know how to write testable requirements to make DREs secure, and NIST's recommendation to the STS is that the DRE in practical terms cannot be made secure. Consequently, NIST and the STS recommend that VVSG 2007 should require voting systems to be of the SI "class," whose readily available (albeit not always optimal) examples include op scan and DRE-VVPAT.

The widespread adoption of voting systems incorporating paper did not seem to cause any widespread problems in the November 2006 elections. But, the use of paper in elections places more stress on (1) the capabilities of voting system technology, (2) of voters to verify their accuracy, and (3) of election workers to securely handle the ballots and accurately count them. Clearly, the needs of voters and election officials need to be addressed with improved and new technology. The STS believes that current paper-based approaches can be improved to be significantly more usable to voters and election officials, and that other kinds of all-electronic IV (software IV) and E2E cryptographic systems may possibly achieve the goal of secure paperless elections. However, for VVSG 2007, the STS judges that designs for these new systems are still immature and that developing testable requirements for these approaches is not yet feasible. Industry has not yet responded in a significant way with new designs, and some method for jumpstarting industry to design and market these approaches may be beneficial.

2.4 The TGDC at a Crossroads

The TGDC is at a crossroads as it develops its security recommendations to the EAC. The TGDC, in arriving at these recommendations, needs to pay attention to issues that can be at times conflicting or in direct opposition, including:

- accessibility,
- reasonable cost,
- usability by voters and election officials, and
- preventing and detecting fraud and error.

It does not help that these issues have aroused much passion in various audiences, some of whom see these issues only in "black and white". Clearly, this is one of the most important decisions the TGDC must make for future voting system directions. The following sections discuss the STS recommendations and other surrounding issues in greater detail.

[6] See http://gaming.nv.gov/stats_regs/reg14_tech_stnds.pdf.

3. The Recommendation for Software-Independent Voting Systems

First, this paper repeats the definition of software-independence: A voting system is software-independent if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome. Conversely, voting systems that are software-dependent have no recourse but to rely on the correctness and integrity of their software in ways that software-independent systems do not. As noted previously, determining whether complex software programs are correct is extremely difficult and in a practical sense infeasible.

It should be noted that in SI, "software" is really means *complex technology*, which can be software implemented on hardware, e.g., burned into PROMs or built into ASICs. "Software independence" should be interpreted to really mean *complex technology independence*.

3.1 Types of SI Voting Systems

There are several types of software-independent systems, however those that are readily available today are paper-based. These are as follows:

1. Op scan using manually marked paper ballots
2. Op scan using an EBM, which can produce a richer user interface including support for accessibility and alternative languages
3. DRE-VVPAT

These systems produce voter-verified paper records and are classified as software independent because their electronic records or counts can be independently audited for accuracy against the voter-verified paper records. Using op scan as an example, a voter marks a paper ballot with her choices and, in the process of doing so, verifies the paper ballot. After the paper ballots are optically scanned, the paper ballots can be used, then, as an audit record to check the accuracy of the scanner's totals.

DRE-VVPAT works in somewhat the opposite way: the voting system creates an electronic record of the voter's choices at a touchscreen device and then prints a summary of the choices on a sheet or roll of paper. The voter can then inspect the paper record to verify its accuracy before finalizing the electronic record, and the paper record remains as an unchangeable voter-verified audit trail that can be used in audits.

It should be noted that how a state chooses to handle discrepancies between the electronic and paper records is outside the scope of the TGDC, but one would expect that it be handled in a way that permits election officials to exercise their full judgment with respect to probable causes, etc. Also outside the TGDC's scope is the question of whether the voter-verified paper record is to be used as the ballot of record in an election. However, as required by states, the paper records should support use as the ballot of record in recounts.

Two types of paperless voting systems that are still immature in their design are:

> *Independent Verification (IV)*: An IV system would have two separate computing machines, a voting machine (VM), such as a DRE, and an audit machine (AM). The voter must verify the ballot at least on the AM. Both create electronic records of every ballot cast, and the two electronic records should be identical; one audits the

other. One sub-class, called *witness systems*, could be conceived as a camera that photographs the voting screen as each ballot is cast.

E2E systems: In an E2E system, a voter gets a receipt with which she can assure herself that her vote is correctly included in the final tally, but cannot prove how she voted to a third party. At the election end, the voter can use her receipt in various ways to check whether her vote was counted. Most approaches are based in cryptography[7], and some researchers believe these systems hold the greatest promise for secure, paperless voting systems.

These systems may be dependent on software to an extent, however not nearly to the extent that today's DREs rely on software correctness. How this software would be specified and tested remains a matter of debate. Currently, the STS is divided on whether software IV systems are possible to secure at this point without further research.

3.2 Relationship to IDV / IV in VVSG 2005

NIST and the TGDC provided an informative discussion for IDV (now called IV) in VVSG 2005. Systems such as op scan and DRE-VVPAT meet the general requirements for IV, those being that the voting system must produce an additional record of its electronic cast vote records in such a manner that the voter can verify the accuracy of the one record independently of the voting system, i.e., the voting system is not able to make changes to the electronic records. IV (IDV) was included in the VVSG 2005 as informative text.

Arguments for or against IV have focused more on issues concerning voter-verification of paper records, e.g., the additional cost of DRE-VVPAT systems, the necessity of the paper audit trail and its usefulness of the paper trail in audits, and issues with the accessibility of paper in general. Used as a primary concept to describe a class of systems, the IV term can detract from what STS sees as the main issue: the difficulty and expense of evaluating complex code and then subsequently trusting t hat it doesn't contain errors or that it has remained secure and tamper-free when fielded. The terms *software-independence* and *software-dependence* better illustrate this issue.

3.3 Auditing in SI vs. non-SI Approaches

The primary issue in the difference between the software-independent and software-dependent classes of systems is the level of auditability. In a software-independent voting system, e.g., op scan, an auditor can always go back to the paper ballots to verify whether the electronic counts are correct. Thus one can determine from an independent audit whether the voting system has recorded the electronic counts correctly. In a software-dependent voting system approach such as the DRE, this is not possible and therefore the correctness of the election outcome relies on the correctness of the software in the DRE.

One of the central themes in the debate over voting system approaches such as the DRE is whether the level of certainty in the DRE is still adequate to ensure that the records have been recorded correctly. With a DRE, one can count the number of people who use the system and then compare this with the number of electronic records; other items can be checked such as number of write-ins or ballot types, and the DRE's event log. While useful

[7] The 3 Ballot voting system is an example of an E2E system that is not based on cryptography. The paper includes an overview of E2E approaches; see http://theory.lcs.mit.edu/~rivest/Rivest-TheThreeBallotVotingSystem.pdf.

in detecting some obvious errors or fraud, these checks do not assure that the records correctly capture the voter's choices. Trust in an election outcome relies heavily upon trusting the correctness of the DRE's software and upon trusting that the DRE software has not been replaced nor tampered with.

But, assuring software correctness and security is very difficult and expensive, and techniques for doing this are still an open research topic. Industry therefore tends to use approaches for detecting errors in software that incorporate comprehensive and independent end-to-end audit trails. Perhaps the most familiar examples are financial systems and customer receipts, but this level of independence in auditing gets repeated in many other areas, including state lotteries and gaming industries. Simply put, the DRE architecture's inability to provide for independent audits of its electronic records makes it a poor choice for an environment in which detecting errors and fraud is important.

3.4 Inability to Test Complex Systems for Errors and Fraud

The need for software-independence in voting systems is based on the inability, in a practical sense, to test complex systems for errors and intentionally-introduced fraud. Software development experts reject the effectiveness of even fairly rigorous development process, reviews, and testing at finding or preventing errors and intentionally malicious code in today's voting systems. Voting systems are increasing in complexity as more features are added, e.g., accessibility functions. In addition, voting systems often use COTS products that are very complex, such as Microsoft Windows CE and Embedded XP. Testing current and future voting systems to a high degree of security would be extremely expensive and most likely not cost-effective for a vendor.

However, arguments persist that most errors are caught by testing and that intentional fraud has not nor will be a major issue in voting system security. Security analyses have proposed that a useful measure of the security of a voting system is the size of the conspiracy required to "rig" a large election, i.e., the larger the conspiracy required, the more secure the system[8]. A software-dependent approach such as the DRE provides no independent capability to detect whether fraud has not caused errors in the records. In principle, a single clever, dishonest programmer in a voting machine company could rig an entire statewide election if the state uses mainly one kind of system (only 4 voting system vendors have a significant US market share).

The arguments to refute the above generally focus on these assertions:

1. there is no evidence of intentionally-introduced malicious code or fraud in voting systems,
2. election procedures are effective at keeping voting systems free of intentionally introduced fraud, and
3. the current testing of voting systems is adequate to uncover intentionally malicious code.

Assertions 1 and 2 do not hold up against the enormous evidence of computer fraud that has occurred in other areas of IT and that has or is likely to occur in voting systems, given the billions spent on elections as well as the rich history of electoral fraud. If a software-dependent voting system such as the DRE cannot be tested to determine whether malicious code exists on the DRE or whether fraud has occurred, then one can't make the argument

[8] See http://vote.nist.gov/threats/index.html and http://www.brennancenter.org/dynamic/subpages/download_file_36343.pdf.

that it hasn't occurred and that election procedures are effective at preventing it. This leaves more approximate estimates of whether fraud has occurred, such as pre- and post-election polling compared with election results. But what if the results differ? If there is no recourse but to recount the electronic records of the DRE, there simply is no recourse. However, elections should not have to rely on approximate estimates of accuracy such as these.

Regarding assertion 3, much evidence has been produced that voting systems in general are not developed according to rigorous models of secure code development nor tested with the rigor of other security-critical applications. Experts reject that even these measures would be sufficient for reliably detecting all errors or malicious code hidden in a voting systems. Various states have now expanded their scrutiny and testing of voting systems.

3.5 Does Use of Paper Make Elections Less Accurate?

A common argument against the use of paper in elections is that the difficulties and inevitable errors that occur in handling and counting paper actually makes elections less accurate than if performed entirely on paperless DREs. Paper can be lost, stolen, or damaged, besides being difficult to handle. Proponents of this argument often cite as an example the current implementations of DRE-VVPAT, which do have significant, but to a certain extent fixable usability issues. But the absence of paper records doesn't necessarily make DREs less error-prone. Also, the auditability of election results is important, therefore it doesn't follow that this should be sacrificed because paper can be difficult to handle. While some paper-based systems such as DRE-VVPAT are ripe for improvement, it appears that the November 2006 elections did not have widespread problems in general with paper-based systems.

Paper has been lost or stolen; it can be switched or otherwise tampered with. Generally speaking, this has occurred when accepted practices and procedures have not been followed. But if people fail to follow accepted procedures, then *any* voting system can become insecure. It is arguable that some state-mandated procedures required to handle and transport paperless DREs safely are even *more* burdensome than the procedures for handling and transporting paper[9].

All the same, more effort should be placed into making paper-based systems more usable and convenient to audit accurately. There is a large amount that can be done in this area, especially with DRE-VVPAT. In an election in which DRE-VVPAT paper trails were at issue, one study[10] showed that the voting system did not print important information on the paper rolls that would be necessary to identify the election, which machine generated the paper roll, and whether one paper roll was a continuation of another paper roll. As well, the vendor did not supply any tools for handling or spooling the paper rolls, thus election officials had to do this by hand. Clearly, improvements can be made and STS is proposing changes in

[9] See, for example, California's procedures, http://accurate-voting.org/wp-content/uploads/2006/11/DESI_AV-TSX_AVPM_Procedures_(2006-05_FINAL).pdf, especially pp. 65-67 and p. 70, and Colorado's court-ordered procedures, http://www.votingintegrity.org/pdf/co_secure-evoting.pdf, especially Sections 1, 5, 6, 8, 9, and 10.

[10] See http://bocc.cuyahogacounty.us/GSC/pdf/esi_cuyahoga_final.pdf and http://www.wired.com/news/technology/0,71999-0.html?tw=wn_politics_evote_5.

requirements for paper-based systems to this effect. Some studies assert that use of EBMs might be a more usable and accessible) approach than DRE-VVPAT, for example[11].

3.6 Can DREs be Improved and Made More Secure?

Are there ways to improve DREs so that they can be made secure and fully auditable? NIST and the STS do not know how to write testable requirements to satisfy that the software in a DRE is correct. The use of COTS software in DREs causes additional problems; having, for example, a large opaque COTS operating system to evaluate in addition to the voting system software is not feasible.

NIST's recommendation to the STS is that in practical terms the DRE's software-dependent approach cannot be made secure or highly reliable. NIST has explored an approach for development of reliable and secure software-dependent DRE-like voting systems patterned after avionics and other industry practices[12], and concluded that major changes would need to be made to voting system development for this, in theory, to result in more secure approaches. Briefly, experience in testing software and systems has shown that testing to high degrees of security and reliability is from a practical perspective not possible. Thus, one needs to build security, reliability, and other aspects into the system design itself and perform a security fault analysis on the implementation of the design. This relates somewhat to the use of the Common Criteria for specifying systems, indeed the IEEE P15.83 subcommittee on voting began a Common Criteria protection profile for specifying voting system security[13]. The steps that would be needed to arrive at a secure software-dependent voting system would likely include the following:

1. Voting systems would have to be built to carefully vetted designs that include precise specifications of control and data inputs/outputs.
2. Voting system vendors would need to follow strict software development processes and prove their abilities to meet other strict standards of management and development.
3. Changes in the way voting systems are certified would be in order, including a requirement to perform fault analyses on the voting systems.
4. Changes in the way voting systems are maintained in the field would be necessary, especially in incorporating a feedback loop to the vendor for reporting errors and problems.

While these changes, in theory, could be made and could yield voting systems that are reliable and secure against certain threats, they would not mitigate the threat of malicious code inserted by an insider at the voting machine company, and other testing would be still required, e.g., OEVT. Whether these changes would work in practice is highly debatable, given the scope changes that would be required.

---

[11] See http://vote.nist.gov/SaltmanRpt20060815.pdf and http://www.wired.com/news/politics/evote/0,71957-0.html?tw=wn_politics_evote_8.

[12] See http://vote.nist.gov/TGDC/Reliability_Reqs_Metrics_Certification20061019.doc.

[13] The IEEE P1583 group is expired; its main page is http://grouper.ieee.org/groups/scc38/1583/. The protection profile was never completed; see http://vote.nist.gov/TGDC/eVotingPP_DRE_v0.13.pdf. http://vote.nist.gov/ecposstatements/MercuriEACmemo.pdf discusses the protection profile.

Given the above factors as well as the difficulty of guaranteeing software correctness, STS recommends that the adoption of software-dependent voting systems on the basis that software errors and fraud can be entirely or mostly prevented is unsound, and that relying on the much stronger audit and detection methods provided in the software-independence class is very well motivated. Software-independent voting systems should support much greater assurance of the correctness of their election outcomes, as there would be fewer and hopefully no lingering unanswerable concern that the election outcome was actually determined by some software bug or a malicious piece of code. It may well be that, because of the expense and infeasibility of testing, the voting industry may have no choice but to adopt software-independent approaches for future voting systems.

4. Current Issues with Paperless SI Approaches

The pursuit of secure paperless SI approaches to voting systems has become an active research goal and has resulted in several commercial devices[14] that to some degree meet requirements of SI. As described earlier, there are at present two types of paperless SI systems: software IV and E2E.

NIST has pursued the goal of writing testable requirements in VVSG 2007 for software IV and E2E systems. NIST has produced several proof-of-concept designs for software IV systems and, with them in mind, attempted to abstract a set of requirements. This has been very difficult for a number of reasons centering on the basic difficulty of abstracting testable security requirements from these several untested designs. As well, there are major concerns about the inherent usability and accessibility of such systems that these designs do not address (e.g., how would users react to a system with not one but two screens?).

NIST asserts that it is possible to design a software IV system that is significantly more secure than a DRE, but probably not as secure as a voter-verified paper-based system. However, standards for these systems would need a period of experimentation and testing. Otherwise, standards written based on unproven research designs would be bound to constrain innovation in such a nascent field.

The STS is divided as to whether it can incorporate high-level requirements for software IV systems in VVSG 2007. An interesting but at this time unanswered question is whether software IV approaches blur the line between software independence and dependence and how far that line can be crossed before the approach begins to look completely software-dependent. For E2E systems, though, the STS does plan to incorporate high-level and possibly more detailed requirements so as to guide development of new approaches.

4.1. The Innovation Class

Requiring SI voting systems in VVSG 2007 effectively leaves only voter-verified paper-based approaches for now. It is important, though, that new and innovative approaches to voting systems be pursued, especially with regard to secure paperless approaches. But, secure

[14] Two paperless commercial approaches to SI include http://www.votehere.com and http://www.democracysystems.com/index.html. Approaches in general are discussed in http://vote.nist.gov/SaltmanRpt20060815.pdf and http://www.cs.umd.edu/~bederson/voting/.

paperless and other approaches are not likely to be pursued by vendors if testable requirements and a certification path for them are not included in VVSG 2007.

STS recommends that a process to encourage the creation and certification of innovative SI approaches (both paper-based and paperless) be put in place. Possibly by stating the high level objectives of these systems in conjunction with other incentives, this may encourage work on innovative systems and developments of prototypes. There would be a need for a defined review process, probably involving a panel of experts and a public review period, to evaluate the security of these systems. STS refers to this approach as the *innovation class*.

The innovation class would be a real path in VVSG 2007 for vendors to submit designs. It should include requirements such as

- strong documentation requirements on the system architecture and security features,
- publicly disclosed source code if the system is software-dependent,
- an expanded OEVT process,
- an open review by a panel of experts, and
- usability, accessibility, and reliability testing.

At least software IV and E2E systems are potential candidates for the innovation class. The security requirements for each may be very different, though. In the case of E2E, there likely will be a cryptographic protocol and one or more algorithms to evaluate. It is conceivable that new interface standards may be required, and perhaps NIST reference implementations.

The innovation class would be an ongoing process and may take some years to produce marketable results. But it constitutes a plausible method for motivating industry to innovate and design new, better voting systems involving both paper and paperless approaches. The innovation class requires more definition from STS and NIST, and final details may best be left to the EAC. STS strongly recommends that this be included in VVSG 2007, though, to encourage researchers and vendors to submit new and innovative designs.

5. Ramifications of Requiring SI

The most obvious ramification of requiring SI in VVSG 2007 is that paperless DREs could not be certified to VVSG 2007. Purchase of paperless DREs would still be permitted, but certification of new paperless DREs would be prohibited after, likely, 2009/2010 when compliance with VVSG 2007 may be required[15]. This effectively leaves only voter-verified paper approaches for certification in the near/foreseeable future, including op scan, EBM devices, DRE-VVPAT, and, possibly, some E2E approaches.

The question of transition plans is a separate question from whether SI should be required in VVSG 2007[16]. The 2007 VVSG would not rescind their existing certification; the 2007 VVSG

[15] The EAC has not announced when voting systems will be required to be certified to VVSG 2007, but it estimates that there will be roughly a 2-year window from when it is announced to when it is required - this will follow roughly the same process as for VVSG 2005.

[16] TGDC Resolution #38-05 states: " ... Although the VVSG was developed based on current best practices and available technology, the recommendation may not include all practices currently followed or technologies currently utilized by election administrators. Consequently, existing practices in some jurisdictions may not be in compliance with the VVSG. The TGDC finds that whether such

would not in itself require existing DRE systems to be replaced. Transition plans may be a policy question that is best left to the EAC and not the TGDC[17].

By default, though, if no transition plan is put into place, systems certified before 2009/2010 will be grandfathered. Unless states decide to adopt stricter rules, systems purchased before that date will continue to be usable in elections. Also, unless states decide to regulate otherwise, systems deployed before that date can continue to be used after that date. However, some policy decisions may need to be made regarding patching of grandfathered systems, which could require certification to the 2007 VVSG.

6. Conclusions and Recommendations

The first conclusion of this paper is that software-independent approaches to voting systems are an effective approach to providing comprehensive and precise audits of voting system records and that they should be required in VVSG 2007. Software-dependent approaches such as the DRE are not viable for future voting systems.

A second conclusion is that development of SI approaches should not stop with current paper-based approaches and the needs of election officials as well as the needs of the accessibility community in dealing effectively with paper should not be ignored. NIST and the TGDC must continue to work on usability and accessibility requirements for systems such as op scan and DRE-VVPAT. There is good reason to believe that much more can be done to make these systems more usable and convenient for voters and for election officials who must audit them. Use of EBM devices may be a more usable and accessible paper-based approach than regular op scan and DRE-VVPAT. STS, with input from HFP and CRT, should continue to write requirements to make paper-based systems more usable, accessible, and easier to audit.

Thirdly, the innovation class is necessary to encourage and promote new and innovative designs for better voting systems, both paper-based and paperless. We need voting systems that the computer engineering and security community can accept as reliable and secure, that election officials can feel are practical for them, and that are sufficiently usable and accessible for voters. This innovation may not occur without a push from government or other sources to make it easier to vet, test, and potentially certify such approaches.

The STS recommendations, then, are as follows:

1. **Require SI voting systems in VVSG 2007:** STS recommends requiring SI voting systems in VVSG 2007 and, conversely, not permitting software-dependent approaches.

2. **Focus attention towards improving the usability and accessibility of paper-based SI voting systems:** HFP and STS should continue to work together to incorporate requirements to make op scan, EBM, and DRE-VVPAT more usable, accessible, and convenient to audit. If this work requires more time than allocated

---

practices or technologies not contained within the VVSG should be "grandfathered" is a policy question not within the jurisdiction of the TGDC, and not within the statutory duties of NIST."

[17] An orthogonal issue that may have some bearing on this matter is whether existing DRE systems may need to be replaced with new voting systems sooner than the standard 10-year lifespan (from VVSG 2005 I.4.3.2).

for VVSG 2007 development, some method for continuing this work should be investigated.

3. **Include high-level requirements in the VVSG 2007 for new approaches to software independence:** Directly testable requirements for E2E approaches are not yet possible, but STS, with HFP input, would include higher-level requirements to guide subsequent development and certification. It remains a matter of debate as to whether high-level requirements for software IV systems can be written at this point without further research.

4. **Foster development of new SI approaches:** STS recommends that research and development of new SI and possibly non-SI approaches be fostered and that an expert panel be created to review approaches. Usability of these approaches should be a primary factor in their design, as well as whether they lend themselves to accessibility.