Report of the Auditability Working Group

Approved by the TGDC for transmittal to the EAC on

January 14, 2011

This document has been prepared by the National Institute of Standards and Technology (NIST) to present the work of the Auditability Working Group of the Technical Guidelines Development Committee. It does not represent a consensus view or recommendation from NIST, nor does it represent any policy positions of NIST.

Certain commercial entities, equipment, or material may be identified in the document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that these entities, materials, or equipment are necessarily the best available for the purpose.

More information can be found at http://www.vote.nist.gov

Report of the Auditability Working Group

TABLE OF CONTENTS

Executive summary

The Auditability Working Group found no alternative that does not have as a likely *consequence* either an effective requirement for paper records or the possibility of undetectable errors in the recording of votes. If undetectable errors can be introduced at any point in the process, then the argument for the correctness of the process as a whole inevitably has a missing link. Optimism that approaching the problem from the auditability perspective would make the "paper or plastic" question go away was based on faulty premises:

- Premise: The risk of undetected error in elections can be handled as a form of audit risk. Fault: Ground truth regarding the correctness of cast vote records comes from the voters alone. After the voters have left the building, votes that were recorded consistently but incorrectly are not detectable by election officials. It is not a matter of detection *risk*—the errors are not detect*able* by any audit. This motivates the creation of cast vote records that are directly verified and independently valid.
- Premise: In the absence of directly verified cast vote records, the practice of dual control can be used to manage the risk of misrecording of votes via independent electronic records. Fault: Dual control is effective at managing risks involving error or fraud by human beings; unfortunately, it is not entirely valid when applied to complex software. Unlike human beings, separately developed pieces of software can share common components, thereby compromising their independence from one another.

Thus, a choice among five mutually exclusive alternatives is presented:

1. Software Independence—robustly mitigates the risk of undetectable error at the cost of effectively requiring paper records with all of the difficulties thereunto appertaining, unless and until a paperless design that satisfies the same requirements is demonstrated.
2. Independent Verification—improves auditability without requiring paper, but certain plausible classes of error remain undetectable.
3. Lossy SI—requires a marginal increase in auditability, but with most of the same costs as Software Independence. Undetectable errors remain plausible.
4. VVSG 1.0—no change. Undetectable errors remain plausible.
5. Hybrid systems—explicitly requires a combination of different kinds of vote-capture devices, where some robustly mitigate the risk of undetectable error while others sacrifice this capability in exchange for providing the best available accessibility.

Once a choice among these alternatives has been made, a set of testable requirements can be derived.

1 Introduction

The Help America Vote Act (HAVA) [1] created the Election Assistance Commission (EAC) to oversee voting standards work. Reporting to the EAC is the Technical Guidelines Development Committee (TGDC), which makes recommendations on voluntary standards and guidelines related to voting equipment. The TGDC in turn created the Auditability Working Group (AWG) to formulate a response to the following charge from the EAC:

> Alternatives to Software Independence (SI)—EAC directs the TGDC to develop draft requirements for audit methods to achieve the goal of Software Independence (SI). The goal is to develop requirements for the auditability of the election system without requiring a specific technology. The starting point for these requirements should be the work already completed by NIST on alternatives to SI.

The TGDC furthermore passed the following resolution at its meeting of July 9, 2010:

- The TGDC charges the Auditability Working Group with the responsibility of drafting a definition of auditability, and what characteristics an auditable system would possess. This definition, and these characteristics, should be developed independently of specific technology and even a consideration of whether or not the technology exists.
- The Auditability Working Group should also prepare a report that evaluates SI, and alternative technology, and their strengths and weaknesses for meeting the auditability objectives.

This report is the AWG's response to that resolution.

2 Defining auditability

2.1 Survey of previous definitions

2.1.1 English

The Oxford English Dictionary Online defines neither the noun auditability nor the adjective auditable. The transitive verb audit is defined as "To make an official systematic examination of (accounts), so as to ascertain their accuracy." [2]

As the dictionary definition reflects, these words are used most commonly, but not exclusively, in a financial context.

2.1.2 VVSG 2.0 (Software Independence)

The August 31, 2007 public review draft of VVSG 2.0 does not define auditability, but the stand-in concept is Software Independence (SI), defined as the quality of a voting system or voting device such that a previously undetected change or fault in software cannot cause an undetectable change or error in election outcome. [3]

Additionally, the glossary of VVSG 2.0 defines the following terms:

> **audit:** Verification of statistical or exact agreement of records from different processes or subsystems of a voting system.
>
> **audit device:** Voting device dedicated exclusively to processes of verification and/or independent assessment of the performance of the voting system.

2.1.3 VVSG 1.0 (Independent Verification)

Predating the emergence of SI as an architectural category, VVSG 1.0 [4] instead refers to Independent Verification (IV). To provide a complete definition of IV, Section C.1.1 of VVSG 1.0 is reproduced below in its entirety.

> Independent Verification is the top-level categorization for electronic voting systems that produce multiple records of ballot selections that can be audited to a high level of precision. For this to happen, the records must be produced and made verifiable by the voter, and then subsequently handled according to the following protocol:
>
> - At least two records of voter selections are produced and one of the records is then stored such that it cannot be modified by the voting system, e.g., the voting system creates a record of voter selections and then copies it to some unalterable media
> - The voter must be able to verify that both records are correct, e.g., verify his or her selections on the voting system's display and also verify the second record of selections stored on the unalterable storage media
> - The verification processes for the two records must be independent of each other and (a) at least one of the records must be verified directly by the voter, or (b) it is acceptable for the voter to indirectly verify both records if they are stored on independent systems
> - The content of the two records can be checked later for consistency through the use of identifiers that allow the records to be linked
>
> An assumption is made that at least one set of records is usable in an efficient counting process such as an automated tabulator, and the other set of records is usable in an efficient process of verifying its agreement with the other set of records used in the counting process. The sets of records would preferentially be

> different in form and thus have more resistance to accidental or deliberate damage.
>
> Given these conditions, the multiple records are said to be distinct and independently verifiable; that is, both records are not under the control of the same processes. As a result of this independence, one record can be used to audit or check the accuracy of the other record. Because the storage of the records is separate, an attacker who can compromise one of the records still will face a difficult task in compromising the other.

Additionally, the glossary of VVSG 1.0 defines the following terms:

> **audit:** Systematic, independent, documented process for obtaining records, statements of fact or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled
>
> **audit trail:** Recorded information that allows election officials to review the activities that occurred on the voting equipment to verify or reconstruct the steps followed without compromising the ballot or voter secrecy
>
> **audit trail for direct-recording equipment:** Paper printout of votes cast, produced by direct-recording electronic (DRE) voting machines, which election officials may use to crosscheck electronically tabulated totals

2.1.4 Other voting references

Three reports by Roy Saltman reflect an evolution in the concept of auditability that mirrors the evolution of U.S. voting systems and practices over the years spanned by the reports.

- In [5], ballot reconciliation, vote reconciliation with undervotes and overvotes, verification of district-wide summations, and recounting are listed as as "aids to audit of calculations." (Most of the audit trail recommendations from these early reports, such as accounting for overvotes and undervotes, are now largely taken for granted as requirements for all new voting systems, and the focus has shifted to harder problems.)
- In [6]: "Two types of audit trails must be distinguished. One type records steps in the operation of computing equipment (both the operation of central equipment by computer operators and the operation of precinct-located equipment by precinct officials). The second type records steps in the execution of the voting process and includes all steps from the printing and distribution of blank ballots, through collection and processing of voted ballots, to the summarization of precinct results."
- In [7], an audit trail is defined as "the retained set of votes cast by every voter individually."

A working group on post-election audits writes, "Two key goals of vote tabulation audits are i) To verify that the election outcomes implied by the reported vote totals are correct, and ii) To

provide data for process improvement: specifically, to identify and quantify various causes of discrepancies between voter intentions and the originally reported vote totals." [8]

A League of Women Voters Report on Election Auditing defines an election audit as "a set of procedures designed to investigate whether an election was conducted properly, the voting equipment counted votes accurately, only qualified voters cast ballots in the election, and the rights of eligible citizens to vote and to experience an efficient and fair voting process were respected." [9]

Post-election audits may include comparing the results of a hand-count of paper records with the totals reported by a voting system (e.g., as described at [10]), but they may also be limited to ballot reconciliation, verification of district-wide summations, and similar operations.

2.1.5 Accounting

The Accounting Terminology Guide of the New York State Society of CPAs defines an audit as "A professional examination of a company's financial statement by a professional accountant or group to determine that the statement has been presented fairly and prepared using Generally Accepted Accounting Principles (GAAP)." [11]

2.1.6 Computer security

NIST IR 7298, *Glossary of Key Information Security Terms*, defines an audit as an "Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures." [12]

The SANS Institute's Glossary of Security Terms defines auditing as "the information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities." [13]

The Windows Server 2003 Glossary defines auditing as "The process that tracks the activities of users by recording selected types of events in the security log of a server or a workstation." [14]

2.1.7 Systems engineering

A stub article in Wikipedia states, "Auditability is a non-functional requirement and concerns the transparency of a system with regards to external audits." [15] It is interesting that this unsourced definition specifies *external* audits, but not the nature of those audits (e.g., financial or security). The auditability article is linked with the subject of systems engineering and an article on the general social/organizational concept of transparency, but includes a "see also" link to the Sarbanes-Oxley Act.

2.2 AWG definition of auditability

Auditability: The transparency of a voting system with regards to the ability to verify that it has operated correctly in an election, and to identify the cause if it has not.

3 Characteristics that an auditable voting system would possess

The following subsections explore different voting system characteristics that logically relate to the auditability of the system. A voting system need not have all of these characteristics to be called auditable; however, requirements for voting system auditability would directly or indirectly mandate some subset of these characteristics.

3.1 Enables detection of errors

3.1.1 Detection through voter verification

A voter reviewing the output of a voting system in any form is able to detect errors in that output. However, the power of this "audit" depends on the relationship of that output to the records of the voting system, the nature and intended use of those records, and whether that output is itself a record. For example:

- Electronic cast vote records can be reviewed only through an electronic interface. Such a review will not reveal a discrepancy between the interpretation that the electronic record is given by that interface and the interpretation it is given in the tally.
- A sighted voter is able to verify that the marks on an optical scan ballot were the marks that the voter intended to make, but such a review will not reveal if the interpretation of those marks by the tabulator is not what the voter intended.

Much work has been done on the properties of different types of voter verification and voter-verifiable records. In the case of ballots, it is frequently argued that direct verification by voters is necessary to provide sufficient assurance that the voting system's records properly record the votes that the voter intended to cast.

To reduce confusion about what sort of verification is intended in different places in this report, the following terms will be used in lieu of the overused term voter verification:

Cast verification: Verification by the voter that a cast vote record, such as a ballot or a VVPAT printout, is consistent with the voter's intent. For example, visual inspection of an optical scan ballot qualifies as cast verification. Cast verification is subdivided into **direct verification**, in which the voter's own senses suffice to inspect the ballot of record (e.g., visual inspection of an optical scan ballot), and **indirect verification**, in which some voting device must intercede to render the ballot into a form that the voter can inspect (e.g., any inspection of an electronic record).

Read verification: Verification by the voter that the interpretation of a cast vote record by a tabulator is consistent with the voter's intent. For example, in an optical scan system, read verification requires that the optical scanner present the voter with an unambiguous representation of the votes that it detected on the optical scan ballot.

Count verification: Verification by the voter that the published election results include the votes from that voter's ballot.

Not to be confused with these terms is Independent Verification (IV), the architectural category of voting systems that was defined in Section 2.1.3.

3.1.2 Detection through independent records

A system may enable the detection of errors using independent records that can be compared against one another for consistency. What constitutes independence (or sufficient independence) is debatable and largely depends on the specific nature and intended use of the records in question.

Ordinary ballot accounting, in which the number of ballots cast is balanced against the number of voters who checked into the polling place and compared with the number of registered voters, is a simple example of an audit technique based on comparison of independent records.

3.1.3 Detection through integrity checks

One form of integrity checking is the validation of input entering the system to ensure that the input is self-consistent and consistent with the state of the voting system. Another form is the creation of additional records, such as digital signatures, that can be used after the fact to test the integrity of the signed records. Each of these techniques enables the detection of certain kinds of errors. However, neither validation of input nor digital signing of records would detect an error where the record created by the voting system was inconsistent with the input from the voter.

3.1.4 Detection through event logging

Inasmuch as errors may be traceable to violations of security policies, improperly executed procedures, or other anomalies, routine operational event logging is an aid to auditing.

3.2 Enables diagnosis of faults

Detecting the existence of errors (e.g., noticing a discrepancy between two totals) is easier than identifying the cause of those errors (e.g., Precinct 5 uploaded unofficial totals with the wrong Precinct ID number). Thus, it is entirely possible for a voting system to be transparent about the existence of errors but opaque to narrowing down what went wrong. A voting system that maintains additional records that are useful in identifying the causes of discrepancies is more auditable than an otherwise equivalent voting system that does not maintain such records.

3.3 Enables correction of errors

Just as diagnosing faults is harder than detecting errors, correcting errors is harder than diagnosing faults. Knowing what went wrong does not ensure that the available records are sufficient to reconstruct the correct answer. While a catastrophe of a magnitude sufficient to destroy every record of one or more ballots is always possible, a voting system that maintains additional records that are useful in reconciling discrepancies is more auditable than an otherwise equivalent voting system that does not maintain any additional records.

To establish high confidence that the reconciliation of a discrepancy is correct, it is generally necessary to locate the cause of the discrepancy and trace its impact so that the correct result can be extracted. In cases where one record is significantly more trustworthy than another, the decision can be taken to discard the less trustworthy record without locating the cause, but to do so calls into question the value of creating multiple records in the first place.

To be worthwhile, a recount must enable the correction of errors in the original count.

3.4 Disambiguates voter intent

Any capability to ascertain the accuracy of a system is compromised if there is intractable uncertainty about what the true or correct result would be under the best of circumstances. One can therefore argue that a voting system that accepts ambiguous inputs from voters is less auditable than an otherwise equivalent voting system that requires voters to commit to an unambiguous representation of their votes when the ballot is cast.

3.5 Preserves records

Audit records must not be intentionally destroyed (e.g., to reclaim storage), nor unintentionally destroyed, nor modified, nor permitted to degrade enough to introduce new errors, for the duration of the retention period that is specified by law. A voting system whose records are prone to deterioration would be less auditable than an otherwise equivalent voting system that creates shelf-stable, archival records. The Voluntary Voting System Guidelines currently in effect already require the memory or media used for storage of voting and audit data to have "demonstrated error-free data retention" for 22 months.

Although the meaning of auditability is different in the jargon of computer security, security is a prerequisite for maintaining the integrity of audit records. The records that are to be used to ascertain the accuracy of the system must themselves be protected from manipulation.

3.6 Supports sampling in post-election audits

Work on small-batch auditing methods has focused on designing post-election audits that demonstrate to a known level of confidence that the winner of an election would not change in a full recount while minimizing the number of ballots that must be recounted to achieve this. [16]

To audit a ballot in this sense generally means to compare an optical scan ballot with the corresponding electronic cast vote record or to manually recount a small batch of ballots and compare the results with a report for that batch.

A voting system that enables the votes from a small batch of ballots or a single isolated ballot to be traced through the system without needing to recount many other ballots in the same geographic or political reporting unit allows a risk-limiting audit to be performed at greatly reduced expense, and is thus arguably more auditable than an otherwise equivalent system that does not support sampling.

A prerequisite for single-ballot auditing is the ability to identify a single ballot. If there are multiple records of a ballot, they must share an identifier to enable the corresponding records to be matched up.

4 Survey of voting system architectures

4.1 Description of architectures

Architectures in current use that need no explanation include optical scan, DRE, and VVPAT. Alternative architectures have previously been explored in [7], in Volume I, Appendix C of VVSG 1.0 [4], and in a NIST report to the EAC [17]. Proposed methods of achieving (or attempting to achieve) auditability without necessarily requiring paper records have included the following:

- The split process architecture. A voting system with a split process architecture consists of vote capture and verification stations that are separate, i.e., two physical devices. A voter inserts an object called a token into the capture station to make ballot selections and then takes the token object to the verification station to review and store the votes. The token object could be paper or unalterable media. Two records of the vote are created: one on the token object and one by the verification station.
- The witness architecture, in which a simple independent verification device passively and indelibly records the same output that is delivered to the voter, e.g., in the form of an archival photograph or audio/video recording, which subsequently can be reviewed without the intercession of the voting system for comparison with the voting system's own records.
- The end-to-end cryptographic architecture, in which there may be only one cast vote record, but there is a way for voters to verify with cryptographic assurance that their ballots were counted in the election totals.
- The audit port architecture, in which the voting system is required to output voting records over a standardized interface to which can be connected any sort of verification device that is compatible. Depending on what is connected, the result could be equivalent to one of the other architectures that was previously discussed.

An additional paper-based variant that was identified in the Auditability Working Group will herein be called Lossy VVPAT, or LVVPAT. LVVPAT is VVPAT except that an independent

voter-verifiable record is generated for only a subset of voting sessions according to a sampling strategy implemented by the voting system itself, and the ability to conduct an audit using that sample is fully supported.

While much could be written about the auditability characteristics of older architectures such as lever machines and punch cards, that discussion would not advance the goals of the present effort.

4.2 Characteristics and comparison

An evaluation of the known modern architectures with respect to auditability and tradeoffs is shown in Table 1.

	Op scan	DRE	VVPAT	LVVPAT	Split process	Witness	E2E crypto	Audit port
Category	SI	non-IV	SI	non-IV	IV	IV	SI	IV
Error detection	Direct verification, post-election audit	Indirect verification, integrity checks, event logs	Direct verification, post-election audit, integrity checks, event logs	Direct verification by a selected sample, post-election audit, integrity checks, event logs	Indirect verification, post-election audit, event logs	Post-election audit, event logs	Count verification	Depends on what connected
Diagnosis	Independent recount (possibly automated)	Contingent on defensive programming and design	VVPAT adds another record but also more points of failure	Less than VVPAT	Multiple devices and token make diagnosis more difficult	If witness device is sufficiently transparent and simple, should help diagnose faults in the other device	No	Depends on what connected
Error correction	Independent recount (possibly automated); no recovery if ballots are unreadable	Duplicate electronic records allow recovery in case records are damaged but no	Reconstruct from VVPAT	Less than VVPAT	Reconstruct from tokens	Reconstruct from witness record	Duplicate electronic records allow recovery in case records are damaged but no	Depends on what connected

	or destroyed	recovery if votes were misrecorded					recovery if all copies fail cryptographic validation	
Vote disambiguation	Requires support for read verification	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Sampling audit	Depends on ballot identification and reporting capabilities	Depends on ballot identification and reporting capabilities	Depends on ballot identification and reporting capabilities	Yes, but sampling strategy should be auditor's prerogative, not determined in advance	Depends on ballot identification and reporting capabilities	Depends on ballot identification and reporting capabilities	Yes (by voters)	Depends on ballot identification and reporting capabilities
Multiple independent cast vote records	No	No	Yes	Only for sample	Contingent on independence of vote capture and verification stations, integrity of tokens	Contingent on the transparency of the witness device	No	Depends on what connected
Persistence of records	Unique paper record	Electronic records with	Both paper and	Electronic records with	Token supposedly	Depends on type of	Depends on specific	Depends on what

	subject to deterioration	back-ups; easier to preserve but also easier to lose	electronic records; some insurance in having different types of records with different modes of failure	back-ups; paper for sample only	unalterable	witness device	design	connected
Security	Protection of the sole record; ballot stuffing, chain voting, etc.	No direct verification; no independent record; requires secure and trustworthy software	VVPAT operational issues may cast false doubt on results	Predetermined sampling limits power of audit	No direct verification; requires independence of vote capture and verification stations, high-integrity tokens; common vulnerabilities of vote capture and verification stations	No direct verification; requires trustworthy witness devices, transparent witness records	Requires correctly implemented cryptography	Depends on what connected, protection of the audit port
Accessibility	Access features difficult to	Wide variety of access features can	Access features difficult to	Not actually improved versus	Depends on form of token. When	So long as the voter is not verifying	Depends on form of voter verification.	Depends on what is connected

	provide from paper ballot; must convert print to alternative forms and eliminate paper handling	be readily provided from digital form of electronic ballot. No paper handling required.	provide from VVPAT; must convert print to alternative forms when VVPAT is or can be ballot of record	VVPAT but possibly more legally defensible since cast verification is not guaranteed to sighted voters[1]	token is paper, access features are difficult to deliver. When token is electronic, access features can more readily be provided but handling of token can still be access barrier. Both vote capture and verification stations must be accessible.	the secondary archival record, no access features would be needed	Whatever media is used by the voter to verify (paper, web site, etc.) would need to be made accessible.	and if the voter is verifying the output of the attached device. Paper output will be more difficult to make accessible than digital output.
Usability	Ballots often marked incorrectly by voters	Potentially best available but depends on user interface design	Usability for audit tends to be poor	Some voters get DRE experience, others get VVPAT experience	Two-stage process may be unintuitive	Same as DRE	Process and added complexity not intuitive to the voter or poll worker	Depends on what connected

[1] A legal review would be needed to determine whether any given LVVPAT design is compliant with the Americans with Disabilities Act and other applicable law. The functionality would need to be implemented in a non-discriminatory way.

Privacy	Current accepted practice	Current accepted practice	Paper rolls record sequence of ballots	An appropriate sampling strategy can improve privacy versus VVPAT	Combined issues of DRE + token (maybe paper) + verification	Potential to record sequence of ballots or (worst case) photograph the voter	Possibly enhanced by obfuscation of choices	Depends on what connected
System complexity (lower is better)	2 (accessible voting station + scanner)	1	2 (DRE + printer) or 3 (+ readback from printout)	3 or 4 (... + overhead of having a variable process for the voting session)	2 (vote capture + verification station)	2 (vote capture + witness device)	2 (vote capture + cryptographic overhead)	Depends on what connected

Table 1 Evaluation of architectures with respect to auditability and tradeoffs

4.3 VVPAT

VVPAT has seen significant deployment as a retrofit to improve the auditability of paperless DREs. It remains of particular interest as a compromise that offers the SI level of auditability combined with the efficiency of electronic voting in what some see a best-of-both-worlds merger. On the other hand, perhaps because of the experience that has been gained from the use of VVPAT in practice, issues with VVPAT have been identified from practically every angle, making worst-of-both-worlds a plausible evaluation as well:

- The addition of an audit trail printer to a DRE adds the complexity of maintaining and operating a printer and managing paper records on top of the existing complexity of managing the DRE itself, nullifying a significant part of the operational advantage that DREs initially offered.
- When an audit trail printer malfunctions, the voter and the DRE won't necessarily notice. Later, the absence of an audit trail for some voting sessions may cast doubt on the election, nullifying a significant part of the trust and confidence advantage that paper audit trails initially offered.
- The usability of VVPAT for audit or recount purposes is reportedly bad, with human error introducing a large number of false discrepancies. [18] The introduction of bar codes to solve this problem is controversial since the content of the bar code is not directly verifiable by the voter.
- With regards to accessibility, the VVPAT that have been deployed thus far do not have the capability to provide an audio verification off of the paper record itself; they can only recite the content of the electronic record on the DRE back to the voter. To implement a scanning capability that would support an accurate audio verification of the content of a paper audit record without reliance on any electronic records would be technically challenging, would require careful design of the paper audit record, and would add to the cost and complexity of the equipment.
- If the capability to provide an audio verification off of the paper record were provided, there is the question of why a blind voter should have confidence that the readback was faithful to the record. This question is analogous to the original question of why any voter should have confidence that the representation of their votes on an electronic display was faithful to the unobservable electronic record in a DRE. One idea is for "observational testing," in which some sighted voters use the audio readback feature and confirm that it is operating correctly—analogous to parallel testing. Another idea is for the paper audit trail to be read by a COTS piece of equipment that is arguably independent of the DRE—analogous to IV. A third idea is that this additional level of "checking the checker" is simply not wanted or needed.
- Some VVPATs were implemented using thermal paper, which degrades rapidly if exposed to heat, light, or solvents. Preserving these records for 22 months is a greater challenge than it is with plain paper ballots.
- VVPAT that is implemented using continuous, uncut rolls of paper preserves the order in which ballots were cast at a voting station. When combined with a pollbook log of voters checking in, the secrecy of the ballot may be partly or completely compromised,

depending on how many voting stations there are and whether the allocation of voters to voting stations can be determined after the fact.

The minimum cost to jurisdictions of following the VVPAT path is significantly impacted by whether the as-yet unimplemented capability to provide an audio verification from the content of the paper audit trail alone is required. In 2003, the Department of Justice responded to an inquiry with an opinion that readback from the paper audit trail was not required. [19] However, that decision was based on the assumption that the paper ballot was merely a contemporaneous record, not an official ballot. Since that time, some jurisdictions have designated the paper audit trail to be an official ballot or a controlling ballot of record used for recount, in which case VVSG 1.0 requires the voting system to enable visually impaired voters and voters with an unwritten language to verify the paper record itself.

No VVPAT devices have entered the certification process since VVSG 1.0 became effective.

4.4 EBM

While VVPAT is a retrofit to make DREs more auditable, Electronically-assisted Ballot Markers (EBMs) could be characterized as an assistive technology add-on to make optical scan ballots more accessible.

For the tasks of navigating through a ballot and marking vote selections, EBMs have the same capabilities as DREs; the level of accessibility that they provide for these tasks is therefore not an issue. However, the accessibility of other tasks associated with the use of EBMs remains a concern.

The interpretation of federal law as it applies to the accessibility of optical scan ballots remains an active and contentious debate with numerous details yet to be ruled on. The eventual cost to jurisdictions that follow the path of opscan plus EBM rather than opscan plus DRE will depend on those rulings. The working group has identified the following EBM issues based on its own understanding of applicable law and requirements, which may or may not be consistent with what is officially determined later:

- An EBM may require a blank ballot of the correct ballot style to be loaded to initiate a voting session; this paper handling step is an accessibility issue. (A similar device that instead prints entire voted ballots onto blank ballot stock, called an Electronic Ballot Printer in the draft VVSG 2.0, avoids this issue.)
- Similarly, transporting a voted ballot to a separate verification station for review, or to a tabulator or a ballot box for casting, requires paper handling. (One or more manufacturers are reportedly developing an EBM device with a scanner attached to it to eliminate that paper-handling step.)
- If voter verification is considered an essential part of the voting process, then verifying the ballot must satisfy the same accessibility requirements as voting the ballot, supporting not only audio read-back, but also accommodations for those using large fonts, high contrast, non-manual input, etc.

- As with VVPAT, to support a proper verification of the ballot of record, the audio read-back must be generated from the votes on the ballot, not recited from memory. However, since in this case the paper record is an optical scan ballot, there is the additional complication of whether ballot text that is ignored by the optical scanner should be ignored by the audio read-back. In jurisdictions where the scanner's interpretation is final, reciting the ballot text from memory (using the same electronically stored ballot styles as the tabulator) would give a more accurate verification; but in jurisdictions where voter intent is determined by direct review, any ballot text that would influence that review should be read back as part of the verification.

4.5 Vote-by-phone

Vote-by-phone is typically used as an accessibility supplement for optical scan or other paper-based voting systems. A voter in a polling place can vote by calling a central service and navigating an audio ballot from a standard land-line telephone. The marked ballot can then be printed or stored in final form as an electronic vote record. In jurisdictions that use optical scan ballot counting, poll workers frequently copy the vote record onto an optical scan ballot to be counted.

Vote-by-phone is not to be confused with remote electronic voting from home or other locations—the voter must still be checked in by poll workers, and all other regular polling place procedures and safeguards apply.

In the absence of additional accessibility supplements, vote-by-phone responds only to the need for non-visual access. The wide range of other accommodations that are supported by DREs and EBMs—simultaneous audio and video presentation, high-contrast and/or large font display, easily distinguishable controls, a range of different input methods—is not available for vote-by-phone. This leaves a significant proportion of people with disabilities either without accommodation or with less than the best accommodation available. Nevertheless, vote-by-phone has been accepted in some jurisdictions as a remedy to bring paper-based systems into compliance with Section 301 of HAVA (e.g., see [20]).

The auditability of vote-by-phone depends on the implementation of the central service. It might or might not create a paper audit trail; it might or might not support an audio readback of that audit trail. One existing implementation supports a mode of operation in which the ballot is faxed back to the location of the voter. If this faxed copy were designated the ballot of record, then direct verification and observational testing would be possible. However, the same accessibility concerns that exist for EBMs and for VVPAT where the paper trail is the ballot of record would then also apply to the verification of this fax received at the polling place.

5 Non-architectural approaches to improving auditability

5.1 Parallel testing

Parallel testing is arguably an audit method that can be used on any kind of voting system. It does not audit the records of the voting system but rather its behavior under test conditions. By carefully controlling those test conditions to deprive the voting system of ways to detect whether it is in a test voting or real voting use, one can gain some confidence that the behavior of the voting system in real voting use should be correct.

Concerns with the effectiveness of the approach center on the feasibility and practicality of depriving the voting system of *any* way to detect whether it is under test. There is an arms race between the complexity of the testing and the complexity of malicious logic that would be needed in the voting system for a software-based fraud to avoid detection.

Since parallel testing is entirely procedural and can be applied to any voting system, it would not result in any new requirements on voting systems in the VVSG. Requirements of the form "The voting system shall not be capable of telling whether it is being parallel tested," while well-intentioned, would be impossible to verify. Thus, from the perspective of making voting systems more auditable, a recommendation for parallel testing would be inert.

5.2 Software assurance

The software assurance alternative does not provide a means to audit the records of the election, but instead tries to reduce the likelihood that an error would be recorded in the first place. The idea is to do whatever it takes for voting system software to earn the trust and confidence of all stakeholders. This may simply be impossible, as trust cannot be forced. However, any approach powerful enough to convince an audience of computer scientists would require invasive and expensive changes to the development process for voting systems, in order to deliver strong evidence that the system as certified and deployed was correct. As a corollary, existing systems that were developed under a different process would no longer be certifiable.

Like Software Independence, software assurance perhaps puts too narrow a focus on software. What is more desirable is an assurance case for the entire voting system, of which software is only one part.

5.3 Innovation class

The August 31, 2007 public review draft of VVSG 2.0 [3] included a provision by which a voting system that achieved Software Independence *without* the use of independent, directly verifiable records could be certified as a so-called "innovation class submission." As the

innovation class is not actually an architecture, but rather a process by which presently unknown, new architectures could be considered, it adds nothing to the alternatives previously discussed.

6 Evaluation of alternatives for VVSG requirements

Attempts to reach consensus on alternatives to Software Independence have been unsuccessful because of conflicting positions regarding requirements for direct verification and the level of risk determined to be acceptable.

6.1 Software Independence

Software Independence is defined as the quality of a voting system or voting device such that a previously undetected change or fault in software cannot cause an undetectable change or error in election outcome. [3]

Computer security specialists who have concluded that software errors and exploits form one of the most critical classes of risks faced by voting systems cannot recommend the use of any voting system that does not mitigate it robustly. Software Independence is phrased as a goal that, when achieved, robustly mitigates that risk.

Direct verifiability of all cast vote records has been most commonly identified as the mechanism to achieve the goal of Software Independence. However, direct verification of paper ballots (optical scan ballots or VVPAT) cannot be done by many voters with visual disabilities and voters lacking fine motor skills or the use of their hands. Voters whose language is unwritten or who are illiterate will also have difficulties with direct verification.

Although the requirement for Software Independence neither specifies a technology nor excludes alternative technologies that achieve the same goal, given currently available technology and the state of the practice, this requirement would encourage near universal deployment of optical scan systems without features that convert complete paper ballot print content into accessible forms or a paper-handling workaround for limited dexterity. Not even strict conformance to the latest proposed VVSG 1.1 or 2.0 would ensure this accessibility. Although gaps and ambiguities in the requirements can be closed, controversial interpretations of the accessibility requirements that were already in VVSG 1.0 have caused the disability community to view the draft requirements and delivery of truly accessible paper-based voting in general with renewed skepticism. To overcome this skepticism, requirements for the accessibility of paper-based voting would need to become significantly more prescriptive to prevent any possible misinterpretation or misapplication of the requirements by system designers and certifiers—a different approach than has been used thus far.

Some election officials feel that the costs of Software Independence are insufficiently justified because risks that are possibly comparable to those that SI mitigates in electronic voting systems have long been tolerated in paper-based systems. For example, voters using central count and manual count paper ballot systems have no direct assurance that their ballots will be protected

from alteration or tabulated as expected. For such systems to have been accepted in practice implies a level of trust in the voting process than is not evident in the rationale for SI. In the absence of a comparable effort to address comparable issues in paper-based voting systems, SI's focus on risks that are specific to electronic voting systems gives the appearance of a double standard of trust.

In response, many computer scientists argue that directly verifiable paper records are inherently more transparent, and therefore inherently more trustworthy, than electronic records. To convince an observer that an electronic record is correct and will remain so, or that an electronic audit record has validity that is independent of the validity of the main cast vote record, is inherently more difficult. It has been said that the purpose of an election is not to convince the winners that they won (as the winners rarely complain), but rather to convince the losers, and their supporters, that they lost fair and square. Software Independence allows the losers and their supporters to confirm that voting equipment operated properly: it gives voters an opportunity to check that the vote-capture equipment recorded their votes as they intended, and it gives observers an opportunity to check that the tabulation equipment counted those records accurately. That observation process does not require trust in software or other complex technology, and can be explained to citizens who are not specialists in information technology.

A decision to require Software Independence would ensure the ability in certified voting systems to audit that votes were recorded as cast. However, unless and until there are accepted ways of achieving Software Independence without direct verifiability, it would come at the cost of reducing the range of voting systems that could be certified to include only those with paper cast vote records, and complicating the accommodation of voters with disabilities. In addition, there would appear to be little incentive for investment in research and development of electronic voting systems absent some commitment of federal resources or new legal requirements. Furthermore, a mandate for paper cast vote records would impact implementation of early voting, super precinct voting and other innovative voting processes that seek to ease access to the ballot.

6.1.1 End-to-end cryptography based systems (E2E)

A review of Table 1 and the definition of Software Independence shows that the only known approach with high potential to achieve Software Independence without the use of paper cast vote records is end-to-end cryptography. Even so, end-to-end cryptography based voting systems are not necessarily free of paper, and research stage systems do not always take accessibility into account.

The draft of VVSG 2.0 provides no clear certification path for end-to-end-systems (only the innovation class process). In that context, end-to-end systems might in some sense be considered an "alternative to SI" that responds to the working group's charge, even though they are assumed to be SI.

6.2 Independent Verification

The Independent Verification concept that was partially developed in the VVSG 1.0 timeframe potentially leads to a less restrictive set of requirements than does Software Independence. A review of the definition in Section 2.1.3 shows that it can be satisfied without paper if two indirectly verified records are stored on independent systems. This implementation path was based on the practice of dual control, which is an internal control that is used in both financial and security contexts. By requiring two independent actors to cooperate in a process, dual control mitigates the risk posed by a single rogue actor and increases the difficulty of committing fraud without being detected. For an obvious fraud to occur, the theory goes, the two actors would need to be in collusion.

However, later work on Independent Verification in the VVSG 2.0 timeframe uncovered different expectations regarding how much independence is necessary to mitigate the critical risks and how such independence could be demonstrated. For example, if it is plausible that the software for two devices that were developed by different manufacturers working in complete isolation from one another could share a dependency on a common COTS library, and that such a library could contain an exploitable fault, then the independence of the manufacturers from one another is ineffective at mitigating the threat posed by faulty library code. Furthermore, since there is no process to certify an incomplete voting system that meets only some of the VVSG's requirements, the independence of separately developed devices would be compromised by the need for them to go through the certification process together. Such problems were the primary reasons that IV was abandoned in favor of SI in the VVSG 2.0 draft.

Lesser reasons included the sense that IV was possibly specifying a solution without identifying the real requirement, as described in the following paragraph from a draft white paper [21]:

> As a primary concept for use in the VVSG 2007, ID/IDV misses the mark in that it describes a technique to achieve software-independence but does not focus on the problem it is attempting to address, that being the inability to verify complex software in voting systems. Consequently, arguments for or against it have focused more on issues concerning voter-verification of paper records, e.g., the additional cost of VVPAT systems and the usefulness of the paper records in audits. We assert that the term *software-dependence* better focuses the argument on the difficulty and expense of evaluating complex code and subsequently trusting that it doesn't contain errors or that the voting system software has not been tampered with.

Some computer scientists raise concerns about the transparency of Independent Verification, arguing that the Independent Verification concept has not been demonstrated to provide meaningful levels of transparency or auditability. A typical observer will not have any good way to confirm whether the equipment provides sufficient independence, and thus no good way to verify that the vote-capture records that were tabulated accurately reflect the voter's intentions. As a result, with Independent Verification, observers have no convincing way to verify for themselves that the voting equipment worked properly. In this sense, Independent Verification

provides less transparency and auditability than Software Independence. Thus, a risk of Independent Verification, compared to Software Independence, is that it could lead to reduced trust in election outcomes. However, Independent Verification would provide more transparency and auditability than paperless DREs.

A secondary risk of Independent Verification is that it may not provide adequate levels of security against sophisticated attacks, such as those based upon viral spread of malicious code.

On the other hand, those election officials who are skeptical that the benefits of SI justify its costs are hopeful that a better balance could be found with paperless approaches to IV. For the kinds of errors that would be detectable by SI but not detectable by IV, the probability of occurrence is debatable; the justification for the added cost and inconvenience of managing paper records is correspondingly weakened. Some therefore see IV as a compromise that would improve auditability without going too far in trying to address threats that are theoretical in nature.

A decision to require Independent Verification as defined, but not required, in VVSG 1.0 would raise the bar for auditability to where a DRE with no independent record could no longer be certified, but it would not "robustly mitigate" the risks posed by software errors and exploits in voting systems.

6.3 Lossy SI

Lossy SI essentially means LVVPAT would be a minimally conforming architecture. "True" SI architectures would also conform, going beyond the minimal requirements.

LVVPAT attempts to avoid overt discrimination against voters with disabilities by randomly denying voter verification to everyone else, rather than by making verification accessible. Compared to VVPAT, LVVPAT does not provide better usability or additional features for any disabled voter, so any accessibility advantage attributed to it would be purely a legal technicality.

LVVPAT does not satisfy the definition of SI or IV; nor does it preserve enough records to enable recovery from a software fault if one is discovered. It does, however, enable a statistical statement of confidence in the results if a sampling audit finds no errors. For assuring the integrity of the electronic records, this is a net gain over what is possible for DREs that have no paper audit trail at all; but the fact that the auditor is not free to select the sample means that the independence of the audit is questionable.

A decision to require a paper audit trail for only *some* voters would draw the line on what is certifiable between LVVPAT and paperless DREs and thereby mandate a marginal improvement in auditability over what is required by VVSG 1.0. However, since VVPAT is simpler and more auditable than LVVPAT, with no genuine difference to accessibility, the only reason to prefer this alternative over SI would be possibly to conserve paper.

6.4 VVSG 1.0

As shown in Table 1, the only modern voting system architectures that would be impacted by a decision between a requirement for Independent Verification and the requirements of VVSG 1.0 are LVVPAT and the paperless DRE.

The main shortcoming of paperless DREs is in transparency and auditability: they do not provide the capacity for observers, or election officials, to confirm for themselves that the voting equipment worked properly in any particular election. As a result, errors and failures of the equipment may go undetected, which can lead to significant undetected errors in the vote tally. This issue has led to an increasing number of change-overs to optical scan or VVPAT despite the DRE's advantages for accessibility and architectural simplicity, and significant sunk costs.

Lacking the market demand, regulatory infrastructure, or resources to develop a new generation of DREs according to a disciplined process of software assurance, parallel testing is the only known approach to mitigating the risks of software errors and exploits in paperless DREs, and there remain concerns both theoretical and practical over the degree to which it can accomplish that goal. On the theoretical side, many computer security specialists are uncomfortable with relying on parallel testing alone as the only defense against these threats because of the limitations that were described in Section 5.1. On the practical side, parallel testing is a procedure that is outside the scope of certification, and the inherent complexity of conducting an effective parallel test puts pressure on election officials to minimize or eliminate that cost.

A decision to keep requirements as they are in VVSG 1.0 would avoid any reduction of the options available to jurisdictions; however, the value of maintaining a standard of auditability that is lower than what most jurisdictions are already requiring on their own is questionable.

6.4.1 Social and political consequences of maintaining the *status quo*

Surveys of the public have shown a significant fraction of the voting population has concerns over the accuracy of computerized voting equipment. [22] The possibility of undetected error in any election is unlikely to reassure those with concerns. Therefore, a risk of continuing to allow paperless DREs is that it is likely to contribute to reduced trust among some segments of the population.

6.5 Hybrid systems

Hybrid voting systems provide two or more different kinds of vote-capture devices in every polling place.

The particular case of providing a single accessible voting station in polling places where voting otherwise takes place using a non-accessible method was specifically allowed in Section 301 of HAVA as a way of making every polling place accessible without requiring immediate

replacement of all existing paper-based voting systems. The accessible voting station could be a DRE, VVPAT, EBM, or vote-by-phone. However, VVPAT and EBM-based hybrids would conform to a requirement for SI, so nothing new would result from discussing them further. To create a separate alternative for VVSG requirements, we must assume that one kind of device would be SI but not necessarily accessible, while another kind would be accessible but not necessarily SI: in other words, a DRE or vote-by-phone based hybrid.

While adding an accessible voting station to an otherwise non-accessible voting system improves accessibility, it is detrimental to the system's usability by election officials, since poll workers then need to be trained in the operation of two completely different vote-capture methods. More generally, the engineering advantage of being able to design different vote-capture devices to match the capabilities of different voters, rather than requiring one device to be all things to all people, is offset by the operational disadvantage of having to deploy and manage more different types of equipment in every polling place.

In terms of transparency and auditability, hybrid systems that use DREs as the accessible voting station offer an intermediate point between paperless DREs and SI. As with LVVPAT, only a subset of voting sessions get a paper record. However, in contrast to LVVPAT, the determination of whether a particular voting session is recorded on paper is made outside the system (preferably, but not necessarily, by the voter).

For vote-by-phone hybrids, unless the fax-back option is implemented, transparency and auditability from the voter's perspective are limited by the fact that all interaction occurs remotely. If a paper record is created only at the central location, the vote-by-phone voter cannot observe it directly. However, depending on implementation details, an audit trail created only at the central location could still yield a stronger capability for internal audits than would be possible for a DRE-based hybrid.

A decision to require a DRE or vote-by-phone based hybrid system, or something equivalent, as a minimally conforming architecture would mean that the VVSG could no longer uniformly require a particular level of performance from all vote-capture devices. It would instead have to require that voting systems be comprised of particular acceptable mixtures of different kinds of devices that meet different sets of requirements. Some jurisdictions might feel that this encroaches on their prerogative to determine the allocation of equipment to polling places.

If it were decided instead to require the lowest common denominator of performance uniformly from vote-capture devices, then in context of the VVSG the entire discussion of hybrid systems would be out of scope. The VVSG requirements would simply remain unchanged from 1.0, and the decision to deploy a hybrid system rather than an all-DRE system would remain a jurisdictional prerogative.

6.5.1 Social and political consequences of the hybrid approach

At a time when the migration of the market was away from optical scan and toward DREs, requiring at least one accessible voting station per polling place in jurisdictions that otherwise

would have had none at all would have seemed a progressive policy. However, in the context of a market that is now migrating in the opposite direction, the exact same voting system leaves many disabled voters feeling segregated and marginalized, particularly if the accessible voting station is used *only* by disabled voters.

A hybrid system in which there was an adequate number of vote-capture devices of both sorts at every polling place, giving all voters the choice, would mitigate the feelings of segregation. Unfortunately, from the perspective of SI supporters, having one non-SI device per polling place would already be a strained compromise, acceptable only because the proportion of voters using the non-SI devices would presumably be small. If the proportion of voters using non-SI devices became significant, the result would be not a compromise, but an effective abandonment of SI.

7 Conclusion

This report has summarized the current understandings of the members of the Auditability Working Group with respect to the definition of auditability, the characteristics that an auditable voting system would possess, and the relative auditability and tradeoffs inherent in the known universe of modern voting system architectures. In addition, it has clarified the impacts of a decision for or against requiring Software Independence, Independent Verification, and several other alternatives. Once a choice among these alternatives has been made, a set of testable requirements can be derived.

8 References

[1] Help America Vote Act of 2002. Public Law 107-252, October 29, 2002.

[2] Oxford English Dictionary Online, http://www.oed.com/, Oxford University Press, July 2010.

[3] Voluntary Voting System Guidelines Recommendations to the Election Assistance Commission, August 31, 2007, http://vote.nist.gov/vvsg-report.htm.

[4] Voluntary Voting System Guidelines Version 1.0 (2005), http://www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx.

[5] Roy G. Saltman, "Effective Use of Computing Technology in Vote-Tallying," NBSIR 75-687, March 1975.

[6] Roy G. Saltman, "Accuracy, Integrity, and Security in Computerized Vote-Tallying," NBS Special Publication 500-158, August 1988.

[7] Roy G. Saltman, "Independent Verification: Essential Action to Assure Integrity in the Voting Process," August 22, 2006.

[8] Correspondence dated 2009-10-29, available at http://electionaudits.org/niststatement.

[9] Report on Election Auditing by the Election Audits Task Force of the League of Women Voters of the United States, January 2009.

[10] Pam Smith and Bob Kibrick, "Manual Audit Requirements," http://www.verifiedvoting.org/article.php?id=5816, July 2010.

[11] "Audit," in *Accounting Terminology Guide*, The Web Site of the New York State Society of CPAs, http://www.nysscpa.org/glossary/term/683, July 2010.

[12] NIST IR 7298, *Glossary of Key Information Security Terms*, April 25, 2006.

[13] "Auditing," in *SANS Glossary of Security Terms*, http://www.sans.org/security-resources/glossary-of-terms/, July 2010.

[14] "Auditing," in *Windows Server 2003 Glossary*, http://technet.microsoft.com/en-us/library/cc736725%28WS.10%29.aspx, updated March 7, 2008.

[15] "Auditability," in *Wikipedia*, http://en.wikipedia.org/w/index.php?title=Auditability&oldid=324628641, as of July 19, 2010, 15:36 GMT.

[16] Small Batch Election Auditing Methods Meeting, https://sites.google.com/site/electionaudits/small-batch, July 2010.

[17] "EAC Research Areas for the TGDC VVSG Recommendations," NIST Voting Team, January 2009, http://www.eac.gov/assets/1/Page/NIST%20Response%20to%20Resolutions%20Adopted%20by%20EAC%20Boards.pdf.

[18] Stephen N. Goggin and Michael D. Byrne, "An Examination of the Auditability of Voter Verified Paper Audit Trail (VVPAT) Ballots," EVT'07 2007 USENIX/ACCURATE Electronic Voting Technology Workshop, August 6, 2007, http://www.usenix.org/events/evt07/tech/full_papers/goggin/goggin_html/.

[19] Whether Certain Direct Recording Electronic Voting Systems Comply with the Help America Vote Act and the Americans with Disabilities Act, October 10, 2003, http://www.justice.gov/olc/drevotingsystems.htm.

[20] United States v. State of Maine (D. Me. 2006) consent decree, http://www.justice.gov/crt/voting/hava/maine_cd.php.

[21] Ronald L. Rivest and John P. Wack, "On the notion of software independence in voting systems," draft white paper, 2006-07-28, http://vote.nist.gov/SI-in-voting.pdf.

[22] "Poll: Voters Want Paper Trail," Wired.com, August 25, 2004, http://www.wired.com/politics/law/news/2004/08/64700.