Draft Chapter on Auditability

Prepared at the direction of the Security and Transparency Subcommittee (STS) of the Technical Guidelines Development Committee (TGDC)

6 March 2007

Chapter 1: Achieving Software Independence Through Audit Steps

1.1 Introduction/Scope

Voting equipment which complies with the VVSG2007 shall support the necessary set of procedures to achieve software dependence.

Software independence means that incorrect behavior of a voting system leading to a change in the results of the election can, in principle, be detected. This kind of incorrect behavior can be detected through the use of good auditing steps; without such steps, the voting system's bad behavior would not reliably be caught. In this chapter, the minimal set of procedures needed to achieve software independence is specified, and requirements imposed by the need to support these procedures are specified for each voting system architecture.

There are broadly two kinds of auditing steps:

- Steps to ensure that all the available records from the voting system agree. These include:
  - Pollbook audit -- verifying that the number of voters for each precinct or election district, and using each ballot style, agrees with the totals reported by the voting equipment. This guards against a voting machine reporting more votes than it had voters, or reassigning some voters to the wrong precinct or ballot style.

- Hand audit of paper and electronic records -- verifying that the voter-verifiable paper records agree with the reported totals from the voting machine. This guards against a voting machine silently misrecording the voter's votes.
- Checking machine records against final tally -- verifiying that the electronic records from the voting machine agree with the final reported totals. This guards against a compromised tally server misreporting the final results.

- Steps to ensure that the voting machine is interacting with the voter properly and recording the votes fairly. These include:
  - Parallel Testing -- isolating some voting machines on election day, and testing them in a way intended to be impossible for the machines to distinguish from normal voting. This guards against the voting machine introducing errors to favor some candidate, omitting choices, skipping races, or simply recording the wrong choice in both electronic and paper records, in hopes that the voter will not notice the contents of the paper record.
  - Spot Parallel Testing -- testing ballot marking devices during the election, by entering choices based on a testing script, and then verifying that the printed ballot correctly represents those choices.
  - Observational Testing -- sending testers who are authorized to vote in an election to cast their own votes, but to do so using assistive technology such as audio ballots. This guards against the voting machine selectively recording the wrong choice on both paper and electronic records when a voter appears not to be able to verify the paper record.

In order to be software independent, each voting system shall support all the steps to ensure that the records agree. VVPAT systems shall support parallel and observational testing; ballot markers shall support spot parallel and observational testing.

The first three auditing steps, intended to ensure the agreement of all available sets of records, are normal parts of current election procedure in many places. Support for these is required of all voting systems; requirements in this chapter provide additional support for these common procedural defenses, and ensure that they can be done in a secure way. The second three auditing steps, intended to ensure the correctness of the voting system's interaction with the voter, are not common election practice, and apply specifically to VVPAT systems and ballot marking devices. Support for these procedural defenses ensures that they can be used effectively.

Support for the full set of auditing procedures described in this chapter imposes a number of different requirements. In order to support the audit steps to ensure that pollbooks, paper records, electronic records, and the final tally from the election are in agreement, extensive requirements on the contents of the electronic records from each voting machine or PCOS scanner, the paper records or ballots used, and the final election tally appear below and in the Electronic Records and VVPR chapters. In order to support the audit steps to ensure that the voting system is presenting choices and recording votes correctly, requirements on the design and behavior of the voting system appear below. Parallel testing imposes the largest requirements of this kind; observational testing and spot parallel testing are much

less difficult to accommodate.

1.1.1 Auditing Procedures Affect Equipment Requirements

The auditing procedures impose requirements for the equipment in three ways:

- Some procedures need specific information or behavior from voting systems in order to be possible or practical. For example, hand-auditing paper and electronic records is only possible if all voting systems produce paper and electronic records that count the same thing.
- Some procedures require certain assurances about the operation of the voting equipment, in order to be meaningful. For example, the hand-audit of the paper and electronic records from DRE+VVPAT systems is meaningful only because the voter is able to view and verify the paper records.
- Some requirements of these procedures raise other potential security problems, which must be addressed by other requirements. For example, electronic records summarizing the votes cast on a given voting machine must be produced in a way that does not violate ballot secrecy.

1.2 Requirements for Supporting Auditing Procedures

This subsection outlines the testable requirements on voting system equipment and documentation for supporting the required auditing procedures.

1.2.1 Pollbook Audit

The purpose of the pollbook audit is to verify that:

- The total number of ballots recorded by the voting system in some location is the same as the total number of voters authorized to cast votes.
- The total number of ballots for each precinct or election district, and for each ballot style, is the same as the total number of voters authorized to vote in that precinct, election district, and ballot style.

This addresses the threat that a tampered voting machine or scanner might have inserted or deleted votes, and also the threat that it may have assigned some voters the wrong precinct, election district, or ballot style to prevent them voting in certain elections or to dilute the effect of their votes.[[Note: This decreases the threat but does not eliminate it.]]

At a high level, the procedure is performed as follows:

- The total number of ballots, and the total number of each distinct type (ballot style, election district, precinct, etc.) is retrieved from the pollbook.

- The total number of ballots, and the number for each ballot style, precinct, or election district, are retrieved from the summary reports produced by the voting equipment. The totals from different machines within one polling place may have to be added together to get counts.
- The numbers are compared, and any discrepancies explained and/or reported.

→ **1.2.1-A** Support for Pollbook Audit

The voting equipment shall support the pollbook audit.

Applies to: *Voting System*

Test Reference:

D I S C U S S I O N

The pollbook audit is critical for blocking some known attacks on voting systems. All voting systems shall support the pollbook audit.

Source: NIST Threats Workshop, Brennan Center Report

Impact:

→ **1.2.1-B** Requirements on Voting System Records and Reports

The voting equipment shall produce records and reports which support the pollbook audit.

- Electronic records produced by each voting machine shall include total number of ballots recorded, and total number of each ballot style and election district or precinct. The voting equipment shall support printing this report. See the Electronic Records section.
- The final election tally report shall include total number of ballots recorded and total number of each ballot style and election district, broken down by polling place. See the Electronic Records section.
- Each paper record or ballot shall include enough information for an auditor to unambiguously determine the ballot style, election district, and precinct without relying on additional equipment.
- Electronic pollbook equipment shall be capable of keeping track of the number of ballots authorized, and the total number authorized of each ballot style, election district, precinct, etc., and of producing and printing a report including that summary information.

Applies to: *DRE+VVPAT, PCOS, Pollbook Software*

Test Reference:

D I S C U S S I O N

The pollbook audit is only practical when the number of ballots, and of each distinct type of ballot, is available from both the pollbooks and the voting equipment. In order to ensure that the number of ballots of each type in the summary report from the equipment is accurate, the same information must appear for each paper record; this permits the hand-audit (see below) to catch discrepancies. Finally, including the number of ballots of each type, broken down by polling place, in the final reported tally from the election allows an auditor to verify agreement between the number of ballots of each type included in final tally, and the number authorized and recorded in the pollbook.

Source:

Impact:

→ **1.2.1-C** Documentation Requirement

The voting system's user documentation shall fully specify a workable and accurate process for producing all records necessary from the equipment and carrying out the pollbook audit.

Applies to: *Voting systems*

Test Reference:

D I S C U S S I O N

In order to fully support the pollbook audit, the voting system documentation must provide enough information for election officials to carry out the auditing step. This includes explaining how to generate all needed reports, how to check the reports against one another for agreement, and how to deal with errors and other unusual problems that come up during the audit step.

Source:

Impact:

→ **1.2.1-D** OEVT Testing

The voting system's documented procedure for pollbook audit shall achieve the critical security requirements of pollbook auditing, even in the face of attack.

- The pollbook audit shall not indicate agreement of number of ballots of each type authorized and recorded, unless these numbers are actually in agreement.

Applies to: *Voting systems*

Test Reference: *OEVT*

DISCUSSION

The process documented by the vendor needs to be checked by the VSTL, both to make sure it works, and to verify that it accomplishes the security goals of pollbook auditing.

Source:

Impact:

1.2.2 Hand Audit of Paper Record

The hand audit of paper record applies to DRE+VVPAT and PCOS voting systems.

All approved voting systems in VVSG2007 produce a voter-verifiable paper record, as well as electronic records from the voting process. The hand audit of paper record procedure verifies that these records are in substantial agreement. This procedure addresses the threats that the voting machine or scanner might record results electronically that disagree with the choices indicated by the voter.

The procedure is done as follows:

- Several polling places or voting machines are randomly selected for auditing.
- The set of races or ballot questions to be recounted is selected.
- For each polling place or voting machine to be audited:
  - The paper records from each polling place or machine to be audited are brought in for counting.
  - The electronic summary record from each scanner or voting machine is printed out.
  - The auditing team hand counts the paper records for the races to be recounted. It also hand counts the total number of paper ballots/records, and the total number for each ballot style.
- The auditing team verifies that its counting results agree with those from the summary report.

➔**1.2.2-A** Support for hand audit of paper records

The voting system shall support the hand audit of paper records.

Applies to: *Voting System*

Test Reference:

DISCUSSION

Hand-auditing paper records to verify agreement with reported electronic records is necessary to detect misbehavior by voting equipment; voter-verifiable paper records offer the voter an opportunity to discover attempts to misrecord his vote on

the paper record, and the hand-audit ensures that equipment that misrecords votes on the electronic record but not the paper record is very likely to be caught.

Source:

Impact:

➞**1.2.2-B** Generic Records Requirements to Support Hand Auditing

The following requirements apply to all voting systems that must support the hand audit procedure:

- The electronic summary record from the voting machine or scanner shall provide all information necessary to hand-audit the paper records, and the equipment shall provide a means to print out the summary records needed to support hand audit. See the Electronic Records chapter for more details.
- The final election tally shall contain all information necessary to hand-audit at the precinct level, and the equipment shall support printing out the summary records needed to support hand audit. See the Electronic Records chapter for more details.
- The paper record of each cast ballot shall include all information necessary to carry out the hand-audit, including:
  - The precinct, election district, and ballot style of this ballot.
- Inclusion of the paper record of a given ballot or ballot summary shall be strong evidence that the ballot was available for review by the voter, and was accepted by the voter.

Applies to: *Voting System*

Test Reference:

D I S C U S S I O N

The electronic summary information from the voting machine or scanner, and the paper records, must contain sufficient information to carry out the hand audit. This means that summaries of the totals from either the voting machines or the final tally must be easy to produce, and that these must be directly usable in carrying out a hand-audit. The hand audit is meaningful only if inclusion of the paper record on the paper roll as an accepted vote summary, or in a ballot box as a cast vote, is strong evidence that the voter had the chance to review the ballot or ballot summary, and approved it.

Source:

Impact:

➞**1.2.2-C** Requirements on DRE+VVPAT paper-roll equipment

The following requirements apply specifically to DRE+VVPAT systems using a paper roll. For more complete requirements, see the VVPR chapter.

- Each paper roll shall identify the voting machine which produced it, the election, and the set of available precincts, election districts, and ballot styles.
- Each ballot record on the roll shall begin with an unambiguous indication of the precinct, election district, and ballot style used. If the ballot is provisional or otherwise needs special processing during auditing or recounts, it shall indicate this in an unambigous human-readable way.
- If multiple rolls are used in a single election, the rolls shall indicate the total number of rolls so far, e.g., “Election 11, District 214, Machine 7991, Roll 2”
- Each ballot record on the roll shall include a clear indication of the voter’s vote on each race on the ballot, including an unambiguous indication of undervotes.
- Each accepted ballot record shall end with a printed indication that the ballot was accepted. This shall be printed when the voter indicates acceptance of the vote.
- Each rejected ballot record shall end with a printed indication that the ballot was rejected. This shall be printed when the voter indicates rejection of the vote.
- Expended paper rolls shall be closed in a container which permits tamper-evident sealing, to protect voter privacy.
- The voting system shall include equipment to support efficient and accurate hand-counting of paper rolls.

Applies to: *DRE+VVPAT with paper rolls*

Test Reference:

DISCUSSION

Paper rolls provide some security and usability benefits in auditing, because a set of ballot summaries are bound together on a single roll of paper. Information identifying the voting machine which produced the records must be placed on each paper roll, to ensure that the hand-audit can determine which machine’s electronic records must agree with the paper records.

Paper rolls also raise many issues. They are very difficult to use in hand-auditing and recounts without special equipment to make this use easier. They store the ballot summaries in order, which places ballot secrecy at risk. The movement of the paper roll into the DRE+VVPAT device is under the control of the DRE, raising the possibility of the DRE accepting or rejecting some ballot summaries without the voter’s approval. The above requirements address these concerns.

Source: NIST Threats Workshop, Brennan Center Report

Impact:

➞**1.2.2-D** Requirements on DRE+VVPAT-cut sheet equipment

The following specific requirements apply to DRE+VVPAT voting systems with cut-sheet paper records. For further requirements, see the chapter on VVPR requirements.

- Each ballot summary shall contain an unambiguous indication of the machine, voting location, and ballot precinct, election district, and ballot style. If the ballot is provisional or otherwise needs special processing during auditing or recounts, it shall indicate this in an unambigous human-readable way.
- A ballot summary shall not be spread across multiple sheets. [[Discuss? This prevents off the shelf printers, which is bad, but not following it would make hand audits potentially difficult.]]
- Each sheet shall contain an unambiguous indication of the voter's vote on each race in the ballot, including an unambiguous indication of undervotes.
- Each accepted ballot record shall include an indication that it was accepted. This shall be printed on the sheet when the voter indicates acceptance of the vote.
- Each rejected ballot record shall include an indication that it was rejected. This shall be printed on the sheet when the voter indicates rejection of the vote.

Applies to: *DRE+VVPAT cut sheet*

Test Reference:

D I S C U S S I O N

Each ballot summary must include all information needed to identify which machine produced it, which type of ballot it is (ballot style, precinct, election district, etc.). All this information is necessary to support the hand-audit. Unambiguous rejection and acceptance markings address the threat that the DRE might attempt to reject or accept ballot summaries without the voter's approval.

Source:

Impact:

➞**1.2.2-E** Requirements on PCOS systems

The following specific requirements apply to PCOS voting systems. For further requirements, see the chapter on VVPR requirements:

- Each printed ballot shall indicate, in human-readable form, all information needed to process it. This includes precinct, election districti, ballot style, provisional status, etc.

Applies to: *PCOS*

Test Reference:

D I S C U S S I O N

PCOS systems are already designed to support recounts.

Source:

Impact:

→ **1.2.2-F** Documentation

The user documentation shall provide directions for a workable and effective hand audit procedure

Applies to: *Voting systems*

Test Reference: *OEVT*

D I S C U S S I O N

The user documentation must explain how to produce all necessary reports and reconcile the paper and electronic records by hand-auditing.

Source:

Impact:

→ **1.2.2-G** OEVT Testing

The voting system's documented procedure for hand audit shall achieve the critical security requirements of hand auditing, even in the face of attack.

- The hand audit shall not indicate agreement of paper and electronic records, unless these numbers are actually in agreement.

Applies to: *Voting systems*

Test Reference: *OEVT*

D I S C U S S I O N

The process documented by the vendor needs to be checked by the VSTL, both to make sure it works, and to verify that it accomplishes the security goals of hand auditing.

Source:

Impact:

1.2.3 Reconciling Machine/Precinct and Final Totals

The purpose of this procedure is to verify that the final reported election tally reflects the totals from each individual scanner and voting machine, plus any additions from absentee ballots, provisional ballots, and other special cases. This guards against the threat that the computer used to produce the final tally might be compromised.

At a high level, the procedure is done as follows:

- The final tally is produced according to the requirements in the Electronic Records chapter. This includes:
  - Totals for each race from each machine which also generated an electronic summary record.
  - Adjustments for provisional ballots and writeins.
  - Totals from machines which did not generate an electronic summary record.
  - Totals from outside sources such as absentee ballots.
- For each machine in the total which produced an electronic summary record according to the Electronic Records chapter:
  - The auditor verifies that the included from the final tally agree with the totals from the machine.
  - The auditor verifies that the included set of ballot styles, precincts, election districts, etc., from each summary agrees with that from the final report.
  - The auditor verifies the digitial signatures.
- For each machine whcih did not produce an electronic summary record according to the Electronic Records chapter:
  - The auditor verifies the agreement of final tally and machine or precinct records using whatever information is available.
- The auditor verifies that the total number of ballots in the adjustments for writeins and provisional ballots either does not change any election outcomes, or is consistent with the number of such ballots indicated in the summary reports.

→ **1.2.3-A** Support for Reconciling Machine Totals and Final Tally

The voting equipment shall support the reconciliation of the machine totals and the final election tally.

Applies to: *Voting System*

Test Reference:

D I S C U S S I O N

This auditing step simply supports the existing canvassing procedure. Every voting system must support this procedure, as it is the only defense against misbehavior by the machine computing the final election tally and producing the report. The Electronic Records chapter includes requirements to make this procedure easier to carry out, and to add cryptographic protection to the records produced by the voting machines. One complication in making a full voting system support this procedure is the likely mixing of old and new voting equipment in a full voting system.

Source:

Impact:

→ **1.2.3-B** Requirements on Voting System Records and Reports

The voting equipment shall produce records and reports which support the reconciliation.

- Electronic records produced by each voting machine or scanner shall include totals for each distinct type of ballot.
- The final election tally report shall include totals broken down by voting machine or scanner, and for each machine/scanner, broken down for each distinct type of ballot. This may leave provisional and write-in votes uncounted (specified only as provisional ballots, counted only as generic write-ins) to preserve privacy.
- The final election tally report shall include total number of ballots, and total number of ballots of each type, for each voting machine or scanner.
- The final election tally report shall be capable of including digitial signature information from the electronic summary records of individual voting machines and scanners.
- The final election tally report shall include adjustments for provisional ballots and write-ins. These need not be linked to specific machines or polling places.

See the Electronic Records chapter for more details on these and related requirements.

Applies to: *DRE+VVPAT, PCOS, Pollbook Software*

Test Reference:

D I S C U S S I O N

This auditing step requires that electronic summary records from voting machines and scanners can be reconciled with the final election tally report. The final

election tally report must thus be capable of breaking down totals by voting machine as well as by precinct.

Source: NIST Threats Workshop, Brennan Center Report

Impact:

→**1.2.3-C** Documentation Requirement

The voting system's user documentation shall fully specify a workable and accurate process for reconciling the voting machine/scanner summary records and the final election tally.

Applies to: *Voting systems*

Test Reference:

D I S C U S S I O N

In order to fully support the audit, the voting system documentation must provide enough information for election officials to carry out the auditing step. This includes explaining how to generate all needed reports, how to check the reports against one another for agreement, and how to deal with errors and other unusual problems that come up during the audit step.

Source:

Impact:

→**1.2.3-D** OEVT Testing

The voting system's documented procedure for reconciling voting machine summary records and the final election tally shall achieve the critical security requirements of the audit, even in the face of attack.

- The audit shall not indicate agreement of voting system summary records and the final election tally, unless these numbers are actually in agreement.

Applies to: *Voting systems*

Test Reference: *OEVT*

D I S C U S S I O N

The process documented by the vendor needs to be checked by the VSTL, both to make sure it works, and to verify that it accomplishes the security goals.

Source:

Impact

1.2.4 Spot Parallel Testing

Spot parallel testing can be done only on ballot-marking devices. The purpose of spot parallel testing is to ensure that a ballot marking device is presenting the ballot correctly to the voters, and is recording the voters' choices correctly. This addresses the threat that the ballot marker could introduce errors in one candidate's favor, skip races, omit choices, or misprint the voter's choices on the ballot.

The procedure is done as follows:

- A set of polling places and machines are selected at random.
- For each machine being tested:
  - The auditor carries out his test during the normal voting time.
  - The auditor makes selections based on a testing script, and has a picture of the full set of ballot choices he should have.
  - The auditor notes any unusual behavior noticed immediately.
  - The auditor brings his note, testing script, and the marked ballot back for analysis as needed.

→**1.2.4-A** Support for Spot Parallel Testing

Ballot marking devices shall support spot parallel testing.

Applies to: *Ballot markers*

Test Reference:

D I S C U S S I O N

Spot parallel testing provides a lightweight alternative to full parallel testing for ballot marking devices.

Source: NIST Threats Workshop, Brennan Center Report

Impact:

→**1.2.4-B** Requirements on Authentication of Voter to Ballot Marker

The mechanism for authenticating the voter to the ballot marking device shall not allow the ballot marker to distinguish testers from normal voters, even with the pollworker's help.

Applies to: *Ballot markers, Pollbook Software*

Test Reference:

DISCUSSION

Spot parallel testing would not detect attacks if the ballot marker were somehow alerted that the tester was carrying out the test. Thus, the authentication mechanism must not permit the machine to discover this fact.

Source: NIST Threats Workshop, Brennan Center Report

Impact:

→ **1.2.4-C** No Networking of Ballot Marker During Voting

Ballot markers shall not permit communications with other devices during the vote collecting process.

Applies to: *Voting systems*

Test Reference:

DISCUSSION

Network connections from other devices to the ballot marker could be used to signal the ballot marker when a spot parallel test was taking place.

Source:

Impact:

→ **1.2.4-D** Documentation Requirement

The voting system's user documentation shall fully specify a workable and accurate process for spot parallel testing.

Applies to: *Voting systems*

Test Reference:

DISCUSSION

Source:

Impact:

→ **1.2.4-E** OEVT Testing

The voting system's documented procedure for spot parallel testing shall achieve the critical security requirements, even in the face of attack.

- The ballot marking device shall not be able to distinguish testers from normal voters, even when the person giving the tester authorization to vote attempts to signal this fact to the ballot marker.

Applies to: *Voting systems*

Test Reference: *OEVT*

DISCUSSION

The process documented by the vendor needs to be checked by the VSTL, both to make sure it works, and to verify that it accomplishes the security goals.

Source:

Impact:

1.2.5 Observational Testing

The purpose of observational testing is to ensure that voting machine is printing a correct representation of the voter's choices on the paper record, even when the voter is using assistive technology. This addresses the threat that the voting machine will misrecord votes on both paper and electronic records when the voter appears unable to verify the paper record.

At a high level, the procedure is done as follows:

- Several election officials and volunteers agree to take part in the testing.
- Each tester is given a full description of the ballot as it is supposed to be presented to him.
- Each tester votes at his normal location, using assistive technology such as audio ballot or screen reader. The tester verifies that the printed version of his ballot is correct.
- The tester reports any problems noted, as well as using the normal process of complaining about malfunctioning machines.

→**1.2.5-A** Support for Observational Testing

Voting machines which interact with the voter to collect votes and support assistive technology shall support observational testing.

Applies to: *DRE+VVPAT, ballot markers*

Test Reference:

DISCUSSION

Blind, low-sight, and some alternative language voters cannot directly verify the paper record produced by the voting system, but must indicate their inability to verify the paper record to the voting machine by requesting an audio ballot, magnified screen images, or other assistive technology. This raises the possibility that a malicious voting machine could steal these voters' votes, by simply recording

the wrong votes on both electronic and paper records. Observational testing provides a defense; a few hundred voters using the assistive technology are also looking carefully at the paper record, and will notice any problem. When observational testing is in use, a malicious voting machine cannot safely assume that a voter using an audio ballot will be unable to check the paper record.

Source:

Impact:

→ **1.2.5-B** Equipment Requirements for Supporting Observational Testing

The following equipment requirements support observational testing:

- The mechanism for authenticating the voter to the ballot marking device shall support observational testing.
- Authentication codes or tokens given to the voter shall not allow the ballot marker to distinguish between testers and normal voters, even when the pollworker is trying to signal the machine of this fact.

Applies to: *DRE+VVPAT, ballot markers, Pollbook Software*

Test Reference:

D I S C U S S I O N

Observational testing would not detect attacks if the voting machine were somehow alerted that the tester was carrying out the test. Thus, the authentication mechanism must not permit the machine to discover this fact.

The requirements on the equipment for supporting observational testing are extremely limited.

Source:

Impact:

→ **1.2.5-C** Documentation Requirement

The voting system's user documentation shall fully specify a workable and accurate process for observational testing.

Applies to: *Voting systems*

Test Reference:

D I S C U S S I O N

Source:

Impact:

➞**1.2.5-D** OEVT Testing

The voting system's documented procedure for observational testing shall achieve the critical security requirements, even in the face of attack.

- The voting machine shall not be able to distinguish testers from normal voters, even when the person giving the tester authorization to vote attempts to signal this fact to the ballot marker.

Applies to: *Voting systems*

Test Reference: *OEVT*

D I S C U S S I O N

The process documented by the vendor needs to be checked by the VSTL, both to make sure it works, and to verify that it accomplishes the security goals.

Source:

Impact

1.2.6 Full Parallel Testing

The purpose of parallel testing is to verify the correct operation of a voting machine. Parallel testing addresses the threat that a voting machine is introducing occasional errors in favor of one candidate, or is presenting the choices in an incorrect way to some or all voters.

The procedure is carried out as follows:

- A few voting machines are randomly selected for parallel testing.
- The selected machines are isolated from all other machines at the polling place.
- The selected machines are subjected to a test election, according to a testing script. The whole test is videotaped, and the voter is
- The results are reviewed and compared with the scripts to detect misbehavior.

➞**1.2.6-A** Support for Parallel Testing

DRE+VVPAT voting machines shall support parallel testing.

Applies to: *DRE+VVPAT*

Test Reference:

DISCUSSION

Parallel testing requires the ability to isolate the voting machine being tested, so that:

- Votes entered into the machine being tested are stored in a separate way from real votes.
- The voting machine is isolated, so that it cannot receive signals from anyone except the testing team.
- The voting machine cannot detect this isolation or separation.
- The voting machine commits to its electronic totals before it is allowed any outside interaction.

Source:

Impact:

→**1.2.6-B** No Networking While Polls Open

The unit of voting equipment to be parallel tested shall not be capable of sending or receiving signals to any machine not either being tested or part of the testing team's equipment during voting.

The unit being tested may include more than one voting machine. However, the whole unit is tested together, with nobody not on the testing team interacting with any machine in that unit, and may have no external communications. Thus:

- If the unit being tested is a single machine, the machine shall not be networked to any other machine.
- If the unit being tested is a judges' station connected to a voting machine, the pair shall not be networked to any other machine.
- If the unit being tested is a small network of voting machines connected together, then that small network shall not be connected to any other machines.

Applies to: *DRE+VVPAT*

Test Reference:

DISCUSSION

If the machine or small group of machines being tested were connected to outside machines under the control of someone other than the testing team, that connection could be used to signal the voting machines that they were being tested, and thus that they should not trigger any malevolent behavior.

Source:

Impact

→**1.2.1-C** No Sharing of Resources

Voting machines and sets of equipment that must support parallel testing shall not share resources such as storage devices or printers, in which any signal or information can flow back from the shared resource to the voting machine.

Applies to: *DRE+VVPAT*

Test Reference:

D I S C U S S I O N

Any shared resources of this kind can allow a covert channel, which would violate the isolation of the voting machine. This has the potential of either allowing the voting machine to learn that it is being isolated (if it is removed from access to the shared resource) or allowing it to receive a signal warning it not to trigger its attack behavior (if it remains connected to the shared resource).

Source:

Impact

→**1.2.6-D** Requirements on Voter Authorization Mechanisms to Support Parallel Testing

The mechanism by which the voter is authorized to vote, and a specific ballot style chosen for him, shall not permit anyone not part of the testing team to alter or control the issuance of authorizations to vote for the machine or machines being tested.

There are two broad requirements on the authorization mechanism:

- The authorization mechanism shall not permit communications of any kind from any person outside the testing team, or machine not being tested, to the machine(s) being tested.
- The authorization mechanism as used by the testing team (as directed in the user documentation for parallel testing support) shall not be possible for the equipment being tested to distinguish from the normal authorization mechanism used in voting.

This leads to the following requirements on specific mechanisms for authorizing votes:

- If authorization is done by physical key, switch, or related mechanism, the testing team shall have access to a copy of the physical key, the switch, etc. The poll workers shall not be part of the authorization process.
- If authorization is done by alphanumeric access code, the testing team shall be capable of generating numerical access codes for the voting machine. Procedural or technical barriers shall prevent testing team

members from using this capability to cast unauthorized votes on other machines in the polling place.

- If authorization is done by rewriteable token, the following requirements apply:
  - The testing team shall be capable of generating a sufficiently large set of rewriteable tokens that the voting machine cannot distinguish this set from the set used in the normal voting process.
  - Normal election procedures shall completely erase the memory of the tokens between uses. The voting machines shall enforce this by failing if they find unexpected information on the token.
  - The testing team may need to bring replacement tokens, and use the set provided for the polling place originally, to avoid alerting the voting machine.
    - Rewriteable tokens used for this purpose should not be reused during a single election, if they contain serial numbers or other identifying information which is available to the voting machines.

Applies to: *DRE+VVPAT*

Test Reference:

D I S C U S S I O N

The mechanism for authorizing voters to vote must be available for the testing team, in order to carry out parallel testing. However, this must not become a mechanism by which the voting equipment is warned that it is being tested.

Source:

Impact:

→ **1.2.6-E** Commitment to Results Before External Communications Allowed

The voting equipment being tested shall commit to its results before it is permitted to connect to any outside device to transmit its results.

The voting machine shall commit to its totals immediately after it is closed down and before it is allowed to connect to any server (even one operated by the testing team) or to have any communication outside the isolated testing environment. This may be done in the following ways:

- A voting machine with a printer may print the summary totals.
- A voting machine with a display screen or a printer may print a cryptographic hash of the machine's summary report. This shall be the same hash value used in the digital signature on the report.

Applies to: *Voting systems*

Test Reference:

D I S C U S S I O N

Source:

Impact:

➞**1.2.1-C** Documentation Requirement

The voting system's user documentation shall fully specify a workable and accurate process for parallel testing.

The user documentation for parallel testing shall include:

- Best practices for parallel testing as specified by [[who? EAC? NIST?]]
- Guidance for testing script generation and an acceptable sample test script.
- Precise steps to be taken to isolate the voting machine without alerting it to its isolation.
- How the commitment to the results is produced before the machine is connected to any outside device or machine.
- How the commitment is to be verified against the electronic records from the voting machine.

Applies to: *DRE+VVPAT*

Test Reference:

D I S C U S S I O N

Parallel testing is a very complicated procedural defense, with many ways it can go wrong. The user documentation for the voting system shall describe in detail how the parallel testing process must be carried out. The VSTL will use this description in evaluating whether the voting system supports parallel testing.

Source:

Impact:

➞**1.2.1-D** OEVT Testing

The voting system's documented procedure for parallel testing shall achieve the critical security requirements, even in the face of attack.

- Once the voting equipment to be parallel tested is isolated according to the procedures given in the user documentation, it shall not be capable of sending or receiving signals or interacting in any way with any machine or person not part of the testing team.

- The isolated voting equipment being parallel tested shall not be capable of discovering, based on what it can observe, whether it is being isolated and parallel tested or is being used in a normal voting process.
- The voting equipment shall not be capable of transmitting different results than those to which it committed before being connected to an outside device, without being detected with overwhelming probability.

Applies to: *Voting systems*

Test Reference: *OEVT*

D I S C U S S I O N

The process documented by the vendor needs to be checked by the VSTL, both to make sure it works, and to verify that it accomplishes the security goals. For parallel testing, this is especially important, as many possible failures of the requirements for parallel testing can only be detected by good open-ended testing.

Source:

Impact