Review of the Documentation of the Sequoia Voting System

Aaron J. Burstein
University of California, Berkeley[1]

Nathan S. Good
University of California, Berkeley

Deirdre K. Mulligan
University of California, Berkeley

July 20, 2007

[1] All author affiliations are provided for identification purposes only.

Contents

Executive Summary

This report examines and evaluates the documentation for the Sequoia voting system that is certified for use in California. This report was prepared as part of the California Secretary of State's "Top-to-Bottom Review" of state-certified voting systems. Our findings complement those three other teams that examined the Sequoia system. These include a source code review team; a "red team," which performed security tests on the Sequoia system's hardware and software; and a team of accessibility experts, which evaluated the system's accessibility to disabled voters. Those teams have submitted separate reports to discuss their findings.

Our review was guided by two overarching questions about the documents. The first question is whether the documentation is ***complete***. In other words, do the documents provided by the voting system vendor contain all the information that election officials need in order to fully evaluate or use the system? The second question is whether the Sequoia system documentation overall is ***sufficient***. That is, how well do all the relevant documents—particularly the technical and user manuals supplied by the vendor—enable the operation of the voting system? This question asks more than whether the documentation will enable the operation of the voting system under ideal circumstances; it asks whether the documentation provides an understanding of the system's overarching properties, and how those properties might be diminished or preserved. In particular, we evaluated the sufficiency of the documentation with respect to the properties of usability, security, ballot secrecy, reliability, and accuracy.

Our key findings are:

1. **The qualification testing reports do not provide enough information to determine independently whether the testing laboratories evaluated the voting system under all applicable voting system standards.**
   The test reports prepared by the three independent testing authorities (ITAs) that evaluated the Sequoia system are incomplete in several major ways. First, one of the ITA reports did not provide any documentation that it had tested the system for adherence to all applicable requirements of the 2002 Voting System Standards (VSS).

   Second, the ITA reports as a whole provide little information about *how* the system was tested to determine its compliance with the VSS. This was manifest in two ways:

   (a) The ITA reports provide scant information about an ITA's methods for testing specific requirements.

   (b) In the case of the AVC Edge direct recording electronic (DRE) voting machine, there are significant gaps in the record of ITA tests. Multiple revisions of the Edge were submitted to the hardware qualification ITA over the course of more than a year, yet there are no preliminary reports from the first six months of the process.

> Without this documentation, it is difficult to know what deficiencies in the system prevented its certification, and how those deficiencies were resolved.

Finally, with one exception, the ITA reports provide no reasoning to support the tester's conclusion that the Sequoia system meets a given requirement.

2. **Typical duties of election officials and pollworkers are not well explained or supported by the documentation.** Documentation for the Sequoia system, though voluminous, often failed to explain procedures clearly and made it difficult to find answers quickly. The documents are also extensively cross-referenced, making it unclear whether an election official or pollworker would have access to a document that he or she would need in order to find necessary information.

   Put simply, the documents are rarely self-contained. During two walk-through elections that we conducted with the Sequoia system, to complete a task we often found it necessary to consult multiple documents, in addition to the documentation for that particular task, in order to answer basic questions. In addition, the documents frequently do not anticipate the potential for error; their value in troubleshooting the Sequoia system was limited. Overall, very few documents were self-contained with respect to any given task in the election process.

   This lack of self-containment is especially serious for the Sequoia Voting System Use Procedures (VSUP) for California. The VSUP appear to be the principal source of guidance for adapting procedures in Sequoia's general documentation to the specific requirements of California law. Yet the VSUP often refer the reader back to Sequoia's general documentation. This seriously undermined the usefulness of the VSUP.

3. **The policies and procedures in the documentation do not provide sufficient guidance about the operational details of voting system security.** The documentation tends to treat voting system security as a topic that is separate from other election administration concerns. We found that this tendency led to significant gaps and inconsistencies in the treatment of security. For example, security procedures are often presented without the context of the particular threats that they are intended to guard against. The documentation also does not discuss the roles of election staff and pollworkers in a unified way, and thus fails to warn that one person should not serve in multiple roles that differ in their levels of access to the voting system. Finally, we found that the documentation does not provide sufficient procedures for handling removable media—particularly re-writable media—in highly security-sensitive facilities, such as central counting and tallying facilities.

Chapter 1

Introduction

Documenting the assembly, maintenance, use, and troubleshooting of a system as complex as a voting system is a difficult task. A single system might combine proprietary hardware, custom operating systems and software, commodity personal computers, and pen and paper. Describing these highly varied components is one function of voting system documentation. But it is not only voting system technology that is heterogeneous; so are voting systems users, and the environments in which the systems are used. Election officials, pollworkers, and voters often need guidance from documents in order to administer or use a voting system. In addition, voting system certification—the process by which a system is approved for use in a state—demands evidence that a voting system complies with one or more sets of standards or guidelines. Documentation provides the details that certification bodies need to evaluate the system. Taken as a whole, voting system documentation must explain the system in several ways to meet the needs of these multiple audiences. All of these demands form a critical part of the background to our review of the Sequoia voting system's documentation.

We submit this report as part of the California Secretary of State's "Top-to-Bottom Review" of certified voting systems. Our work began on May 31, 2007 and concluded with the submission of this report on July 20, 2007.

1.1 Scope and Methodology

Reviewing voting system documentation does not lend itself well to a single, rigidly specified method. In order to develop an approach that was consistent with other document review teams participating in the Top-to-Bottom Review, we stayed in close contact with them throughout the project. To develop a document evaluation framework, we first turned to the 2002 Voting System Standards,[1] as well as the California Elections Code and state regulations. These sources specified some necessary types of documentation. They also provided us with a roadmap of an election; we attempted to develop a comprehensive list of election phases, beginning with certification of the system and concluding with the system's use in post-election audits and recounts. Initial passes through the documents provided a sense of their range and allowed us to determine, roughly, to which election phases a given document would most be most rele-

[1] Federal Election Commission, Voting System Standards (2002), *at* http://www.eac.gov/election_resources/vss.html.

vant. This also gave us a sense of the intended audience for each document. We also turned to members of the Source Code Review and Red Teams for consultations throughout the review. Finally, we used the documentation to conduct two days of "walk-through" elections on the Sequoia system.

The ultimate questions that we sought to answer in this review were whether the Sequoia documentation is ***complete*** and whether it is ***sufficient***.

The question of completeness concerns whether we had all of the documentation from the vendor would give to election officials to allow them to evaluate or administer the system. The types of documents involved are national-level evaluation test reports, state evaluations and certificates, technical documentation of the system, operators manuals, and training materials.

Whether the documentation is sufficient is a question of how well it helps the intended reader (a voter, election official, or pollworker) accomplish what he or she needs to do with the voting system. Thus, sufficiency may be a matter of degree. In some cases, a document might be self-contained, providing all information necessary to to perform some task. In other cases, the desired information might be scattered throughout several documents, requiring a potentially extensive search and synthesis. Finally, we did not consider the sufficiency of the documentation only in the context of concrete, discrete tasks. We also considered whether the documents were sufficient to accomplish five overarching properties of the voting system: usability, security, ballot secrecy, reliability, and accuracy.

Our review began on May 31, 2007, and concluded with our submission of this report on July 20, 2007.

1.2 Limitations of Our Study

Though we reviewed all documentation and had some time to use the Sequoia equipment, we are aware that our review is incomplete in a few significant ways. Perhaps most importantly, it was outside the scope of our review to consider jurisdiction-specific documents and procedures. In many areas of this report, we have had to qualify our findings with the recognition that jurisdictions may have procedures in place or documents available to address concerns that arose from the documents that we reviewed.

Perspective is another limitation. It inescapable that we are not election officials or state voting system examiners, and do not bring their experience with voting system and election administration to our reading of the system documentation.

Another limitation of this study is that the documents we reviewed might not be the documents that participants in the election system actually use. For example, jurisdictions might substitute their own documents, such as pollworker training materials, for the documents that we reviewed.

Finally, the timeframe for the review was compressed; we are certain that we have touched on or omitted some issues that would benefit from a more extended analysis. For example, we did not have time to take an in-depth look at event logs and other types of data that are used in post-election auditing.

1.3 Summary of Findings

For several of these properties, we found that the documentation, even when complete, is insufficient. In particular: This report examines and evaluates the documentation for the Sequoia voting system that is certified for use in California. This report was prepared as part of the California Secretary of State's "Top-to-Bottom Review" of state-certified voting systems. Our findings complement those three other teams that examined the Sequoia system. These include a source code review team; a "red team," which performed security tests on the Sequoia system's hardware and software; and a team of accessibility experts, which evaluated the system's accessibility to disabled voters. Those teams have submitted separate reports to discuss their findings.

Our review was guided by two overarching questions about the documents. The first question is whether the documentation is ***complete***. In other words, do the documents provided by the voting system vendor contain all the information that election officials need in order to fully evaluate or use the system? The second question is whether the Sequoia system documentation overall is ***sufficient***. That is, how well do all the relevant documents—particularly the technical and user manuals supplied by the vendor—enable the operation of the voting system? This question asks more than whether the documentation will enable the operation of the voting system under ideal circumstances; it asks whether the documentation provides an understanding of the system's overarching properties, and how those properties might be diminished or preserved. In particular, we evaluated the sufficiency of the documentation with respect to the properties of usability, security, ballot secrecy, reliability, and accuracy.

Our key findings are:

1. **The qualification testing reports do not provide enough information to determine independently whether the testing laboratories evaluated the voting system under all applicable voting system standards.**
   The test reports prepared by the three independent testing authorities (ITAs) that evaluated the Sequoia system are incomplete in several major ways. First, one of the ITA reports did not provide any documentation that it had tested the system for adherence to all applicable requirements of the 2002 Voting System Standards (VSS).

   Second, the ITA reports as a whole provide little information about *how* the system was tested to determine its compliance with the VSS. This was manifest in two ways:

   (a) The ITA reports provide scant information about an ITA's methods for testing specific requirements.

   (b) In the case of the AVC Edge direct recording electronic (DRE) voting machine, there are significant gaps in the record of ITA tests. Multiple revisions of the Edge were submitted to the hardware qualification ITA over the course of more than a year, yet there are no preliminary reports from the first six months of the process. Without this documentation, it is difficult to know what deficiencies in the system prevented its certification, and how those deficiencies were resolved.

   Finally, with one exception, the ITA reports provide no reasoning to support the tester's conclusion that the Sequoia system meets a given requirement.

2. **Typical duties of election officials and pollworkers are not well explained or supported by the documentation.** Documentation for the Sequoia system, though voluminous, often failed to explain procedures clearly and made it difficult to find answers quickly. The documents are also extensively cross-referenced, making it unclear whether an election official or pollworker would have access to a document that he or she would need in order to find necessary information.

   Put simply, the documents are rarely self-contained. During two walk-through elections that we conducted with the Sequoia system, to complete a task we often found it necessary to consult multiple documents, in addition to the documentation for that particular task, in order to answer basic questions. In addition, the documents frequently do not anticipate the potential for error; their value in troubleshooting the Sequoia system was limited. Overall, very few documents were self-contained with respect to any given task in the election process.

   This lack of self-containment is especially serious for the Sequoia Voting System Use Procedures (VSUP) for California. The VSUP appear to be the principal source of guidance for adapting procedures in Sequoia's general documentation to the specific requirements of California law. Yet the VSUP often refer the reader back to Sequoia's general documentation. This seriously undermined the usefulness of the VSUP.

3. **The policies and procedures in the documentation do not provide sufficient guidance about the operational details of voting system security.** The documentation tends to treat voting system security as a topic that is separate from other election administration concerns. We found that this tendency led to significant gaps and inconsistencies in the treatment of security. For example, security procedures are often presented without the context of the particular threats that they are intended to guard against. The documentation also does not discuss the roles of election staff and pollworkers in a unified way, and thus fails to warn that one person should not serve in multiple roles that differ in their levels of access to the voting system. Finally, we found that the documentation does not provide sufficient procedures for handling removable media—particularly re-writable media—in highly security-sensitive facilities, such as central counting and tallying facilities.

Chapter 2

Description of the Sequoia Voting System

The Sequoia voting system provides three ways to cast and tally ballots. The AVC Edge is a direct recording electronic (DRE) voting machine used in precincts. The Optech Insight is an optical scan machine that processes paper ballots cast in precincts. Finally, the 400-C is a central-count optical scanner; it is used to process paper ballots in a central location in a jurisdiction. Each of these devices depends on a number of other devices and software applications, which we describe in more detail along with the relevant equipment. Also of central importance to the Sequoia system is WinEDS, the election management system.

2.1 WinEDS

As the Sequoia system's election management system, WinEDS is, in effect, the brain that that coordinates all the functions of the voting system. WinEDS manages all phases of the election process, from defining ballots, to preparing machines for use in each of a jurisdiction's precincts, to tallying ballots and reporting results after an election. WinEDS is a software application designed to run under recent versions of the Microsoft Windows operating running on commodity PC hardware. WinEDS is installed with the Microsoft Office Suite, which is used to create and process results reports. WinEDS is a complex application that handles highly sensitive election data. Procedures issued by the California Office of the Secretary of State require WinEDS to be used in a secure facility under the supervision of the registrar of voters.[1]

WinEDS can be used on an isolated workstation; or it may be configured to work on a networked client-server model, with each client serving a specific function, such as tallying or preparing memory cartridges. To facilitate this multi-user model, the WinEDS machine comes preconfigured with 10 different roles, and allows for workstation-, user-, and role-based security. WinEDS can operate with all, some or none of these features enabled, providing a great deal of flexibility.

Prior to an election, a technician enters information about the election into WinEDS. This information includes not only the definitions of each race or ballot question, but also the serial number of each AVC Edge and Optech Insight, as well as the precinct to which each machine

[1] Memorandum from Bruce McDannold, Interim Director, California Secretary of State Office of Voting System Technology Assessment, to All users of Sequoia voting systems, Oct. 20, 2006 ("OVSTA Memo").

is assigned. WinEDS is used to define the election, including information about each race and ballot question. Once this information has been entered, WinEDS is used to define ballots. These definitions, in turn, are copied to memory cartridges and MemoryPacks for use in the AVC Edge and Optech Insight, respectively. Additionally, WinEDS is used to configure the HAAT and Card Activator units that will be used to activate vote cards for Edge access. See sections 2.2-2.3 for further details.

After an election, WinEDS is used to tally ballots cast on the Edge, Optech Insight, or 400-C. WinEDS can also generate a wide variety of tally reports. Once WinEDS is in the tally phase, it prohibits changes to basic election information, such as the contest and candidate data.[2] If a jurisdiction uses multiple WinEDS workstations, then each WinEDS system can be assigned specific roles during the tally phase. For example, one PC could be used to tally results, while the other PC could be used to view the tally in real time[3].

To tally results from the precinct-based Edge and Optech Insight, WinEDS reads the removable ballot data storage media from each device. In some jurisdictions, the results media are removed in the precincts and transported to a secure central location. In other jurisdictions, the results media are kept in the voting machines. WinEDS reads the Insight's MemoryPacks via the MemoryPack Reader, which connects to a WinEDS workstation through a serial port. Results from the Edge are contained on Results Cartridges, which are compact flash memory cards with a PCMCIA hardware interface. The election reports generated by WinEDS and can be exported to a variety of common word processing, spreadsheet, and database formats. WinEDS comes preconfigured with reports for looking at security logs, election results, and other portions of the election process that WinEDS manages.

Version information:[4] WinEDS 3.0.12.

2.2 Optech Insight and Optech Insight Plus

The Optech Insight and Insight Plus (referred to collectively as Insight throughout the remainder of the document) are optical scanners classified as vote tabulating devices under California Elections Code § 358.[5] The Insight is an in-precinct scanner. Accordingly, it is designed to provide feedback to voters in the form of rejecting ballots that contain overvotes and providing warnings about undervotes.

The Insight comprises the hardware program system (HPX), which is stored on a programmable read only memory (PROM) chip in the Insight itself, and the application program system (APX), which is stored on the MemoryPack. The MemoryPack device has three principal parts: random access memory (RAM) for recording election results; flash memory to

[2] WinEDS Election Data System Reference Guide for Software Release 3.1 5-3, 6-3, rev. 6.02, Jan. 2006 ("WinEDS Reference Guide").

[3] WinEDS Reference Guide at 6-3.

[4] The version number for WinEDS is the version that is part of the certified Sequoia system. The version information following the descriptions of other components in the remainder of this chapter is analogous.

[5] According to Cal. Elec. Code § 358, a vote tabulating device is a "piece of equipment, other than a voting machine, that compiles a total of votes cast by means of ballot card sorting, card reading, paper ballot scanning, electronic data processing, or a combination of that type of equipment."

store ballot definition files and precinct identifiers; and a separate flash memory area to store the APX application software.[6] The MemoryPack contains a battery to power the RAM—and thus preserve stored ballot images and other vote data—in case power to the Insight is interrupted. Before an election, each MemoryPack is programmed by the WinEDS server to carry the ballot definition files appropriate for the precinct in which that MemoryPack will be used. These ballot definition files prepare the optical scanning hardware to interpret marked ballots. In addition, each MemoryPack carries with a precinct identifier, which links MemoryPacks and the corresponding ballot definition files to the precincts (and ballots) with which they are to be used. Once a MemoryPack has been programmed, it is inserted into the assigned Insight and sealed with a serialized, tamper-evident seal by the registrar of voters (or his or her staff); and the serial number is logged. Insights equipped with MemoryPacks inserted are delivered for use in precincts on election day.

Version information: Optech Insight/Insight Plus, APX K2.10, HPX K1.42, Memory Pack Reader (MPR), firmware version 2.15.

2.3 AVC Edge I & II

The Sequoia AVC Edge is a direct recording electronic (DRE) voting system.[7] The California Secretary of State has certified two models of the Edge Models I and II. Since both Edge models run the same firmware and share the same documentation, this report refers to "the AVC Edge" or simply "the Edge."

The AVC Edge is primarily used to to record votes on election day in precincts. The Edge provides overvote protection by preventing a voter from selecting more candidates than allowed under the ballot definition. The Edge may also provide undervote warnings, though its behavior is configurable.

The AVC Edge has a 15-inch LCD touchscreen that displays the ballot; allows voters to make selections and navigate the ballot; and provides an interface for testing, maintenance, and opening and closing the polls. On the front of each Edge unit is a slot for a smart card (also known as a "vote activation card"). A voter must have an activated smart card in order to begin voting. After the voter casts his or her ballot on the Edge, the smart card is deactivated and returned to a pollworker. This prevents one voter from voting multiple times.

The back of the Edge contains the power switch and a switch that opens and closes the polls on that particular voting machine. The cover for the poll function switch accommodates a tamper-evident seal. Also on the back of each Edge unit is a yellow "Activate" button, which can be used to switch the Edge into different operating modes. Finally, the backside of the Edge has a small LCD screen (two rows of 20 characters) that displays diagnostic and error messages. Sequoia uses a proprietary operating system for the Edge.

Similarly, the firmware that the Edge uses to control the hardware and to allow voting are proprietary applications. The Edge also contains three serial EEPROMs (electronically pro-

[6] Optech Insight Plus Hardware Specification § 2.3.1, rev. 1.01, Sept. 2005.

[7] *See* Cal. Elec. Code § 19251(b), which defines "direct recording electronic voting system" to mean "a voting system that records a vote electronically and does not require or permit the voter to record his or her vote directly onto a tangible ballot."

grammable read-only memory), which store permanent configuration information about the Edge unit as well as ballot counters. One of these EEPROMs is the "configuration ROM," which holds information to identify the machine and the customer and also contains a "cryptographic seed value." The other EEPROMs hold a public counter (a counter that is reset at the beginning of each election) and a protective counter (a counter that is incremented each time a vote is cast and is never reset).

The ballot definition and audio files to assist visually impaired voters are programmed on a WinEDS election management system server and stored on the Results Cartridge. Prior to an election, the Results Cartridge is inserted into the Edge's Results Port and covered by a plastic door, which is sealed with a tamper-evident seal.

The Results Cartridge also stores the Audit Trail, which consists of ballot images, ballot summaries, and the event log.[8] The Edge also stores a copy of the Audit Trail in the internal Audit Trail memory. If the Results Cartridge is lost, damaged or destroyed, it can be recovered from this internal memory.[9]

Event logging for the Edge is always turned on; it cannot be disabled.[10] At the close of an election, a pollworker may print the audit log on a VVPAT. Alternatively, or in addition, election officials may access the event log stored as part of the Audit Trail on the Results Cartridge.

Several other devices support the Edge. First, the Card Activator processes the smart cards (also known as "vote activation cards") that voters use to access the Edge.[11] After each use of a smart card, the Card Activator prepares the card for use by another voter. Before an election, each Card Activator must be prepared with the ballot definitions and other information appropriate for the precinct in which it will be used.

An alternative to the Card Activator is the HAAT (Hybrid Activator, Accumulator, and Transmitter). There are two models of the HAAT, Model 50 and Model 100. Currently, only the HAAT 50 is certified for use in California.[12]

Finally, the VeriVote printer attaches to the Edge to allow printing of a voter-verified paper audit trail ("VVPAT"), as required by California law.[13] Security seals on the VeriVote's enclosure protect the paper trail against tampering. In addition, there are security seals to prevent the VeriVote printer from being detached from the Edge.

Version information: AVC Edge I/II, firmware version 5.0.24; Card Activator, version 5.0.21; HAAT Model 50, version 1.0.69L; VeriVote printer.

[8] AVC Edge Release 5.0 System Overview § 2.13, rev. 1.00, May 10, 2005.

[9] *Id.* § 2.15.

[10] AVC Edge System Manual § 2.14.

[11] The Edge can also be configured to run in "manual activation" mode. This requires a pollworker to reset the Edge after each voter.

[12] The principal differences between the HAAT 50 and the HAAT 100 are: (1) the HAAT 100 has a printer; (2) the HAAT 100 has a cellular phone modem, which allows it to transmit unofficial results at the close of an election; (3) the HAAT 100 can be used to consolidate results from multiple Edges at the close of an election; and (4) configuration files for the HAAT 50 can only be loaded via one of its USB ports, while the HAAT 100 can use either the USB ports or the PCMCIA slot. HAAT (Hybrid Activator, Accumulator & Transmitter) Operations & Maintenance Manual § 2.5, rev. 1.09, Jan. 2006.

[13] Cal. Elec. Code § 19250(d).

2.4 Optech 400-C

The Optech 400-C is a high capacity scanner that is classified as a vote tabulating device under California Elections Code § 358.[14] It is used by election officials to count ballots in a central location. Ballots are cast in precincts and placed in ballot boxes. The ballots are then delivered by two poll workers to the central count facility, where they are fed by an election official into the 400-C. Because it is used by election officials in a secure, central location, the 400-C does not provide voters with feedback about ballot problems.

The system consists of a high-capacity scanner linked to a PC running Microsoft Windows. The 400-C uses a proprietary tabulation program, WinETP, to process the ballots that it scans.[15] WinEDS is used to configure the ballot definition files and precinct identifiers that instruct the 400-C's as to how to interpret each ballot voter's ballot marks. The ballot definitions are then transferred from WinEDS to the 400-C via removable media, such as USB sticks, DVDs, or floppy disks.

When the 400-C is done tallying the results for the election, the results are copied from the 400-C onto a DVD or a memory cartridge and transferred to the WinEDS server. The WinEDS server combines these results with those from any Insight and Edge units used in the jurisdiction. Finally, WinEDS generates tally reports for the election.

Version information: Optech 400-C/Win-ETP, firmware version 1.12.4.

[14] Cal. Elec. Code § 358 defines a vote tabulating device to mean a "piece of equipment, other than a voting machine, that compiles a total of votes cast by means of ballot card sorting, card reading, paper ballot scanning, electronic data processing, or a combination of that type of equipment."

[15] Optech 400-C System Overview § 7, rev. 1.01, Jan. 2005.

Chapter 3

Completeness of Documentation

This chapter provides an overview of the documentation that we received and reviewed for the Sequoia system. After cataloging and describing at a high level the major categories of documentation, we provide a detailed analysis of a key type of documentation: the qualification test reports from the independent test authorities (ITAs) that evaluated the Sequoia system for compliance with the 2002 VSS. We find that the system documentation is incomplete. In particular, at least one of the ITA reports does not provide evidence that the ITA tested all applicable requirements of the VSS.

3.1 Overview

These documents were provided:

- Independent testing authority (ITA) reports from Wyle (hardware and firmware), Ciber (WinEDS), and Systest (HAAT). Parts of these reports were supported by hardware tests performed by subcontractors, whose reports on these tests were also provided to the team.

- Technical data packages (TDPs), as defined in VSS Vol. II, § 2.1.1.1. Documents in the TDP include a system overview; security overview; functional, hardware, and software specifications; and a test and verification specification.

- Operator and maintenance manuals; and training and reference materials for election officials and pollworkers.

The Office of the Secretary of State also provided the Document Review Team with copies of the following public documents:

- California state certifications, Secretary of State staff reports, volume testing reports, and consultant reports for the Sequoia system.

- Memorandum from Bruce McDannold to Sequoia users regarding Sequoia use procedures, which we refer to throughout this report as "the OVSTA Memo."[1]

[1] *See supra* note 1.

In addition, the Document Review Team referred to a number of laws, regulations, standards, and publicly accessible documents:

- The Help America Vote Act of 2002 and the Voting Rights Act of 1965.
- The California Elections Code and related regulations in the California Code of Regulations, title 2, division 7; and the California Government Code.
- The California Voting System Requirements, issued by the Secretary of State in October 2005.
- California state certifications, Secretary of State staff reports, volume testing reports, and consultant reports.
- The 2002 Voting System Standards.
- The Voting System Use Procedures for California Template.

Finally, we note that we did not have access to certain kinds of documents.

- The WinEDS Operators Manual for the Optech Insight. Not having this manual prevented us from learning more about programming MemoryPacks for the Insight. The Source Code Review Team was also affected.
- ITA test plans.
- Penetration analyses prepared by Sequoia or on its behalf. These analyses are listed as references in several ITA reports, but the Sequoia documentation notes that they are available only upon "special request." Ideally, all Sequoia system reviewers would have had access to these analyses. In the future, the Secretary of State should consider requesting them as part of certification or review.

3.2 The Sequoia ITA Reports

3.2.1 Background

Independent testing authorities' (ITA) evaluations of voting systems play a central role in voting system certification. A voting system containing a DRE must have "federal qualification" before the Secretary of State may certify the system for use in the state.[2] At the time the Sequoia system was certified in California (March 2006), ITA reports were the basis for

[2] *See* Cal. Elec. Code § 19250(a) ("On and after January 1, 2005, the Secretary of State shall not approve a direct recording electronic voting system unless the system has received federal qualification and includes an accessible voter verified paper audit trail."); § 19251(d) (defining "federal qualification" to mean that "the [voting] system has been certified, if applicable, by means of qualification testing by a Nationally Recognized Test Laboratory and has met or exceeded the minimum requirements set forth in the Performance and Text Standards for Punch Card, Mark Sense, and Direct Recording Electronic Voting Systems, or in any successor voluntary standard document, developed and promulgated by the Federal Election Commission, the Election Assistance Commission, or the National Institute of Standards and Technology").

national-level qualification decisions by the National Association of State Election Directors (NASED).[3] The source of technical standards under which the Sequoia system was qualified by NASED was the 2002 Voting System Standards (VSS).[4]

ITA reports provide unique insight into how voting systems are designed and function. ITAs have access to voting system source code, documentation, and hardware, a combination of resources that would facilitate thorough assessments of voting system security and other properties. Because few ITA reports have been made public, a detailed review of the ITA reports for the Sequoia system is warranted.

3.2.2 Sequoia ITA Reports: Issues in Common

There is no single ITA report for the Sequoia system. Instead, there are reports from the three ITAs that tested the Edge and related components: Wyle Laboratories, Ciber, Inc., and Systest Labs tested components from the Sequoia system. Wyle tested the AVC Edge DRE and all related components except the HAAT, which was tested by Systest. Wyle also tested the Optech Insight, Insight Plus, and the 400-C. Ciber tested WinEDS.

A significant division is between a "hardware ITA" and a "software ITA." In addition to testing hardware, a hardware ITA tests "firmware"—the software that resides on voting equipment used inside a polling place. A software ITA evaluates other types of software, such as the election management system that a jurisdiction typically uses to process official results after an election.[5] The course of testing by an ITA has three principal parts: functional testing, environmental testing (operational and non-operational), and source code review.

ITA reports, whether for hardware or software testing, tend to share a few features. Narrative descriptions of the tests conducted and the reasoning that the ITA applied to reach its conclusions are usually in the first part of the report. Next, there is a requirements matrix that derived from the 2002 VSS. For each requirement in the matrix, the ITA notes whether the application was tested and, if so, whether the system met the requirement. Only one of the ITA reports that we reviewed provided space next to each requirement to allow the tester to give comments regarding his or her conclusion.[6] The ITA reports also list the elements of the technical data package (TDP) submitted to the ITA, as well as a statement that it reviewed the TDP's contents. Finally, it is common for part of a voting system to undergo multiple rounds of revision and retesting by an ITA. In the case of the AVC Edge, for example, it appears that this DRE and its peripheral devices were revised and re-submitted 24 times before NASED quali-

[3] Since this time, the U.S. Election Assistance Commission (EAC) has taken over responsibility for voting system certification at the national level. This new certification regime also involves a different structure for test lab supervision; NIST, rather than NASED, recommends accreditation for test labs to the EAC. Accredited test labs are now known as voting system test labs rather than ITAs. Because the Sequoia system was qualified by NASED and certified prior to the EAC's taking charge of federal voting system certification, however, we refer to test labs as ITAs.

[4] On December 31, 2007, the 2005 Voluntary Voting System Guidelines will become the guidelines for federal certification. At that time, "[a]ll previous versions of national standards will become obsolete." U.S. Election Assistance Commission, Voluntary Voting System Guidelines, http://www.eac.gov/vvsg_intro.htm (last visited July 15, 2007).

[5] For a thorough explanation of these terms, see Carolyn Coggins, *Independent Testing of Voting Systems*, 47 COMM. ACM 34 (Oct. 2004).

[6] This was the case for Systest's examination of the HAAT.

fied it. In the documents that the Document Review Team had, these revisions were sparsely documented, making it difficult to track the changes over time.

3.2.3 AVC Edge ITA Report

Sequoia AVC Edge firmware version 5.0 was submitted to Wyle on February 1, 2005.[7] The Document Review Team did not receive a report for the qualification testing of that firmware version or of several revisions that followed. The earliest test report we had, however, was for firmware version 5.0.14, dated August 16, 2005 (“the 5.0.14 Report”).[8] Thus, we do not know the reasons for which the Edge had to be modified and resubmitted, nor do we know what changes Sequoia made to the Edge between the initial submission and the 5.0.14 Report. This 5.0.14 Report is described as a “hardware qualification testing” report, while the test reports that follow are described as “Change Release Reports.” The last of these change release reports is for firmware version 5.0.24 and is dated February 8, 2006. NASED qualified the Sequoia system including Edge firmware version 5.0.24 on March 17, 2006.[9] The California Secretary of State certified this system on March 20, 2006.[10]

The 5.0.14 Report references a number of other AVC Edge reports, system documentation, and testing standards. Although the title of this report mentions only “hardware,”[11] the report actually includes an evaluation of the Edge’s firmware – that is, the computer programs that reside on the voting system’s hardware.[12] There is no separate assessment of the Edge’s software by a “software ITA”; the source code review performed by Wyle was the basis for the Sequoia system’s NASED qualification.

The initial sections of the 5.0.14 Report describe the voting system and summarize the kinds of tests that the ITA (and its contractors) performed. The qualification test findings are presented in two forms: a summary narrative description that states the purpose of the test as well as the ITA’s conclusion, and a functional testing matrix.[13] Each row of the functional matrix contains a VSS requirement, indicating the functional requirement that was tested, and four checkboxes to indicate the tester’s conclusion: accepted, rejected, N/A, and N/T.[14]

[7] 5.0.14 Report at B-3.

[8] Hardware Qualification Testing of the Edge Models I & II DRE Voting Machines, VeriVote Printer, Card Activator, and ADA Audio Adapter Peripherals (Firmware Version 5.0.14).

[9] NASED Qualified Voting Systems – FINAL at 28, March 9, 2007, *at* http://www.nased.org/Copy%20of%20NASED%20Qualified%20Voting%20Systems%20FINAL%20030907.pdf.

[10] California Secretary of State, Approval of Use of Sequoia Voting Systems, Inc. DRE & Optical Scan Voting Systems, March 20, 2006.

[11] *See supra* note 8.

[12] *See, e.g.*, VSS Vol. I, § 1.3 (“Qualification testing (in-depth source code review and functional tests) was limited to the firmware and hardware used at the precinct level and did not include any election management software, which typically resides on a personal computer and is used for ballot definition, absentee, and report canvassing activities.”); *id.* § 6.4.1.

[13] A similar matrix appears in the Systest’s qualification testing report for the HAAT. These matrixes are, in turn, similar to a template that appears to have been authored by NASED and these three ITAs, based on the fact that all of their names appear at the top of what appears to be an exemplar for the matrix. *See* Requirements of the FECVSS 2002 Trace to Vendor Testing and Technical Data Package, rev. 04.

[14] We were unable to find a definition of N/A and N/T. Based on the context in which these abbreviations are used, we assumed that N/A means “not applicable,” i.e., a particular requirement does not apply to this part of the Sequoia system; and that N/T means “not tested,” i.e., the requirement applies this part of the Sequoia system but

One of the VSS requirements in the 5.0.14 Report is marked as "rejected": This is the entry for VSS § 2.5.3.1.d, which relates to printing consolidated results reports.[15] No further explanation is provided, though the report for firmware version 5.0.21 notes: "Corrected instance of consolidation cartridge verifying with errors in vote consolidation."[16]

In terms of source code review,[17] the ITA evaluated the Edge's software for readability, understandability, modularity, robustness, security, maintainability, consistency, documentation, usability, and flow control.[18] Much of the source code report consists of a file-by-file analysis of files that differed from the previous submission or were "otherwise noteworthy."[19] It is difficult to characterize the overall substance of this analysis, but many of the comments in this section of the report fall into one of the following categories:[20]

- Changes in variable names relative to the previous firmware revision.
- Program flow control.
- A lack of comments in the source code.

The ITA concluded that firmware version 5.0.14 was not compliant with the VSS.[21] Still, the 5.0.14 Report's Functional Requirements matrix notes as "accepted" every software-related requirement that the ITA found to be applicable and tested.[22] The Report notes, for example, that changes from the previously certified version of the Edge firmware (version 4.3.320) "sometimes introduced FEC issues where none existed before, and other times brought issues into view that had not been noticed before."[23] The Report does not elaborate on what these "issues" were, except to say that "[t]he many issues that were observed in the code" are listed in the file-by-file analysis. Finally, the 5.0.14 Report states that the change log "did not accurately list all the changes" in the source code relative to the previous version.

The Change Release Reports for revisions leading up to the certified firmware version do not shed any more light on the "issues" noted in the 5.0.14 Report. In the months between August 2005 and March 2006, Sequoia submitted the AVC Edge at least four revisions to the Edge system (including the certified 5.0.24 version that was ultimately certified). The report for revision 5.0.21[24] "recommended that this release be considered compliant with the FEC

was not tested by this ITA. The use of the N/T mark appears to track differences in the requirements tested by a hardware versus software ITA, but neither this explanation, nor any other, is given in the documentation.

[15] VSS Vol. I, § 2.5.3.1.d in its entirety reads:

> Produce a consolidated printed report of the results for each contest of all votes cast (including the count of ballots from other sources supported by the system as specified by the vendor) that includes the votes cast for each selection, the count of undervotes, and the count of overvotes.

[16] Change Release Report of the Edge Models I & II DRE Voting Machines, VeriVote Printer, Card Activator, and ADA Audio Adapter Peripherals (firmware version 5.0.21) § 6.1.1, Jan. 5, 2006.

[17] 5.0.14 Report at B-3.

[18] 5.0.14 Report at B-3.

[19] 5.0.14 Report at B-3.

[20] These categories closely track those in the "Assessment of Coding Conventions" section of the VSS. *See* VSS Vol. II § 5.4.2.

[21] 5.0.14 Report at B-19.

[22] *See* 5.0.14 Report at A-23-A-26 and A-27-A-31.

[23] *Id.*

[24] This was the first revision after 5.0.14 for which the Document Review Team had a report.

guidelines for coding practices."[25] For reasons not explained in the available documentation, however, there were three more submissions. In each of the reports leading up to version 5.0.24, the ITA recommended that that version "be considered compliant with the FEC guidelines for coding practices."

Several categories of information were missing from the AVC Edge ITA reports. First, the only functional requirements analysis matrix is in the 5.0.14 Report. This makes it impossible to determine whether additional requirements were "rejected" in previous versions and how they were resolved. A second, and related, type of information missing is an explanation for the sole rejected requirement in the 5.0.14 Report. This report also lacks any explanation of why a given requirement was determined to be not applicable, or why the ITA did not test it. Third, the available documents did not explain why a given version of the AVC Edge was judge not to comply with the VSS. For example, a letter from a Wyle official to Sequoia states that firmware version 5.0.22 was "found to be in compliance with the 2002 Voting System Standards coding guidelines;"[26] yet Sequoia submitted two more revisions before attaining certification. The documents simply do not state who determined that further revisions were required, or the reasons that they were needed.

3.2.4 WinEDS ITA Report

The WinEDS ITA report[27] report describes the testing performed to demonstrate that WinEDS meets or exceeds the requirements for election systems under the FEC 2002 Voting System Standards (VSS). The WinEDS ITA report describes the results of several different evaluations of the WinEDS software, namely a source code review, a document review of the TDP documentation and a functional test of the WinEDS software. The documentation states that the test is intended to discover issue and defects in the software design and operation that could result in failure to complete an election in a satisfactory manner.

The purpose of the source code review was to review the the code's compliance with the VSS. The standards are described as being created to insure "logical correctness, system integrity, reliability and accuracy" of the voting system. In addition to FEC standards, the ITA report reviewed the source code with reference to Sequoia coding standards. The ITA report lists the software components, version numbers, file names, sizes, modification dates, and paths of all of the source documents that were delivered to CIBER for review. In the findings section, the ITA report describes issues they discovered with the software that they reviewed. These findings describe formatting and software code standard issues such as "indenting is inconsistent" and "code needs in line comments." Based on their review process, the CIBER ITA found that the WinEDS 3.1.012 source code meets the standards required by the FEC 2002 VSS.

The functional test review described tests on two configurations of WinEDS software. One configuration consists of the WinEDS software running on a Microsoft Windows XP machine,

[25] 5.0.21 Report at A-12.

[26] Letter to Paul Terwilliger, Sequoia Voting Systems, from Dawn K. Bates, Contract Manager, Wyle Laboratories, Jan. 24, 2006.

[27] Ciber, Inc., Software Qualification Test Report: Sequoia WinEDS 3.1.012, Feb. 15, 2006 ("WinEDS ITA Report").

and one installation running on a Windows 2003 server machine.[28] The database server was Microsoft SQL Server with Service Pack 3a.[29] Both of these installations were described as being tested using end-to-end tests to provide a regression test of the WinEDS software. In order to test the functionality of the system, it is necessary for it to interact with the other portions of the Sequoia election process. WinEDS was tested with the 400-C, Edge I and II, Card Activator, Optech Insight and Insight Plus, and HAAT components. In an appendix, the ITA report describes the test procedures used to run each test. Each test procedure described the voting machines used, the election parameters defined, the election configuration used and then listed the actual test procedures. Two tests were run based on the beginning of the ballot definition stage, the other six tests were run starting from importing the election definitions. The CIBER ITA states that based on their functional test review both installations meet the requirements of the FEC 2002 VSS as well as additional requirements "stated or derived from the TDP."

The CIBER ITA report states that based on the system passing the three tests they performed, they recommend the Sequoia WinEDS 3.1.012 be certified.

3.2.5 Optech 400-C ITA Report

The ITA report for the 400-C consists of a description of tests performed by Wyle Laboratories on the 400-C to meet the requirements of the FEC VSS 2002. The documentation describes the ITA as performing functional tests, electrical and environmental tests, volume testing, and, finally, a source code review of the 400-C firmware[30]

The electrical and environmental tests subject the 400-C to conditions such as extreme temperature changes, humidity, power surges and disturbances, vibration testing and electrical Fast transients.[31]

Functional tests consisted of testing the 400-C against a list of functional requirements such as voting system security, accuracy, integrity, error recovery and audit records.[32] The functional test also included testing compliance with requirements pertinent to a variety of election day activities, including accurately recording vote selections, resumes operation after power interruption, and maintaining the integrity of vote data after encountering an error condition.[33]

The 400-C ITA also describes the volume test. The exact conditions for this test are not clear. According to § 6.2 of the report, "a test ballot containing 92 positions was cast 16,800 times, resulting in an excess of 1,540,000 positions accurately recorded." The report does not provide the test ballot layout. The report does not state how many actual vote selection configurations were tested; it is unclear whether the ballots were identical or were marked differently. Finally, the report does not state whether the ballots were marked by machine or by hand.

[28] WinEDS ITA Report § 5.3.

[29] *Id.* § 3.

[30] Wyle Laboratories, Inc., Preliminary Test Report: Hardware Qualification Testing of the Sequoia Optech 400-C Ballot Counter (firmware version 1.12.4), Jan. 12, 2006 ("400-C ITA Report"). The copy of the report that we were given is unsigned.

[31] 400-C ITA Report, *supra* note 30, §§ 6.4-6.6.

[32] *Id.* at A-3 - A-5.

[33] *Id.*

The source code review was performed on the 400-C's firmware. Similar to other ITA source code reviews, the source code review performed by the Wyle ITA listed the source files, size and dates. Additionally, they provide a list of source code files and comments with line numbers where they found issues with the source code. Issues discovered with the source code consisted of formatting and software coding standard issues such as "uncommented declarations", "single character variablename" and "function headers of functions of greater than ten lines in this file were inadequate". The ITA review of the version 1.10.2 indicated that the "code was not compliant with FEC guidelines for coding practices as set forth within the FEC Performance and Test Standards for Punchcard, Marksense and Direct Recording Electronic Voting Systems."[34] The ITA report notes that the revised 1.10.3 code addresses many of the issues outlined in their initial assessment of 1.10.2 code, yet was still not compliant with FEC guidelines. The ITA report states that Versions 1.10.4 addresses issues from the previous reviews, and is recommended to be compliant with FEC guideline for coding practices as set forth within the FEC Performance and Test Standards for Punchcard, Marksense and Direct Recording Electronic Voting Systems.[35] Revisions 1.10.5-1.12.1 were considered compliant by the ITA. Revision 1.12.2 was considered non compliant, based on bug that would cause windows to crash. The subsequent 1.12.2 version received with a minor revision was considered compliant. The final version reviewed in the ITA, 1.12.4 was considered compliant as well.[36]

The ITA report states that based on the test performed, the 400-C meets the hardware qualification test requirements as described in the April 2002 FEC Voting System Standards. The report states that "any anomalies encountered during the hardware qualification testing were successfully resolved prior to test completion."

3.2.6 Optech Insight ITA Report

The Insight ITA report was also performed by Wyle and was similar in format to the 400-C ITA. The documentation describes the ITA as performing functional tests, electrical and environmental tests, and finally a source code review of the Optech Insight firmware[37] The functional test consisted of activities to simulate a variety of election day activities, such as counting ballots, verifying the machine's correctness, and recovering from power interrupts or other possible problems. For example, the functional test looks at functions such as "the system identifies device failures" as well as "A record of the voters selection of candidates whose names do not appear on the ballot, if permitted under State law, and record as many write-in votes as the number of candidates the voter is allowed to select" in addition to other functional requirements. In addition, the functional test consisted of logic and accuracy tests performed on a variety of ballot types to test the machine accuracy.

The source code review was performed on the Optech Insight's firmware. Similar to source code review performed on the 400-C, the source code review performed by the Wyle ITA listed the source files, size and dates. Additionally, they provide a list of source code files and comments with line numbers where they found issues with the source code. Issues discovered with

[34] *Id.* at 74.

[35] *Id.* at 84

[36] *Id.* at 89.

[37] Wyle Laboratories, Inc., Hardware Qualification Testing of the Sequoia Voting Systems Optech Insight Precinct Ballot Tabulator, Nov. 9, 2005 ("Optech ITA Report").

the source code consisted of formatting and software coding standard issues such as “naked constants”, “multiple exit points” and “function exceeds 120 lines in length”. The ITA report comments that “overall the assembly code was the best commented, most readable assembly code reviewed thus far”. However, the initial version reviewed (HPX 1.32) contained violations of FEC guidelines, namely, a GOTO statement and multiple instances of multiple exit points. The subsequent revisions 1.38 was also deemed non compliant as well. The subsequent revision APX_K2.04/CPX_K1.12/HPX_K1.38 was deemed compliant by the ITA after addressing previous issues. The code versions CPX_K1.13, CPX HPX1.41, May 19, 2005 HPX1.41, APX K2.08, July 1 APX K2.08, HPX K1.42, August 4, 2005 APX K2.08 and finally the August 26, 2005 APX K2.08 be considered compliant with the FEC VSS 2002 guidelines as set forth within the FEC Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems.

The Wyle ITA report states that based on the test performed, the Optech Insight meets the hardware qualification test requirements as described in the April 2002 FEC Voting System Standards.

3.3 Summary

To summarize, the ITA reports that we reviewed were incomplete in two important ways. First, we did not receive all of the incremental reports issued in conjunction with the submission of revised versions of the Sequoia system. Second, we did not have the test plans, which are extremely helpful to understanding how an ITA performed its qualification testing.

Based on the available ITA reports and other documentation, we also find the ITA reports insufficient to understand the specific conclusions that the test labs reached regarding the Sequoia system’s compliance with the 2002 VSS.

Chapter 4

Sufficiency of Documentation

This chapter discusses the sufficiency of the Sequoia documentation with respect to a number of critical voting system properties. Put simply, would the documentation, on its own, allow the relevant participants in the voting system (election officials, pollworkers, technicians, voters) to do what they need to do?

Though we sought to determine whether the documentation as a whole is sufficient with respect to the five voting system performance characteristics, we found it convenient to separate usability from the other four (security, ballot secrecy, reliability, and accuracy). The question of whether the documentation is usable frequently hinges on whether it allows, say, a pollworker to close the polls properly. Thus, the focus in this case is on discretely defined tasks performed by a person holding a readily identifiable role (e.g., a pollworker). In contrast, the other voting system properties that form the basis for our evaluation span multiple election phases and often involve the actions of more than one kind of actor. For example, to determine whether the documentation was sufficient with respect to security, we analyzed whether the documentation would: allow election officials to understand (and develop mitigations against) potential threats; provide clear procedures specifying how to maintain physical security and chains-of-custody throughout the election cycle, provide guidance about how to maintain the integrity of election data; and provide guidance about how to audit the voting system.

We find that the Sequoia documentation as whole is not sufficient, for the reasons that we discuss in the remainder of this chapter. We discuss the usability dimension of document sufficiency first, followed by security, ballot secrecy, and accuracy.

4.1 Usability

We assessed whether the Sequoia documentation was usable on two levels. First, we determined whether, by searching all available documents, we could find sufficient information to complete a specific task. We deem this condition “basic sufficiency.” Second, we determined whether the document(s) that seemed most relevant to a particular task contained sufficient information to make the voting system usable. A document that meets this conditions is “self-contained.” The self-containment condition is more stringent than basic sufficiency.

4.1.1 Method and Goals

The document review teams for all three systems in the Top-to-Bottom Review determined early on that it would be extremely difficult, if not impossible, to determine without actually using the machines whether the documents were sufficiently usable. Thus, we arranged for some limited time to use the voting systems that were housed at the Office of the Secretary of State during the course of the review.

The Sequoia Document Review Team conducted two of these "walk-through" sessions. The goal of these sessions was to accomplish major pre-election and election day tasks by following the instructions in the relevant documents. These tasks included:

1. Defining an election and the corresponding ballots;
2. Loading ballot definitions on the voting machines;
3. Conducting pre-election logic and accuracy testing (LAT);
4. Opening the polls, casting votes, and closing the polls; and
5. Tallying ballots.

The equipment that was available for our use included:

1. AVC Edge I and II DREs,[1] PCMCIA memory cards and vote activation cards, a Card Activator, and two HAAT 50 units.[2]
2. Optech Insight and Insight Plus precinct count optical scanners, multiple memory packs, a Memory Pack Reader and writer, and blank paper ballots; and
3. a 400-C central count optical scanner and blank paper ballots.

Overall, we found that the documents contained insufficient information to make the system usable. This was often the case because the documentation as a whole simply did not contain information that we found necessary to complete the tasks we had set out. A related observation is that the documents sometimes offer little help when the equipment does not behave exactly as it should. Other times, we found the documentation insufficient because documents were internally contradictory, or because key documents contradicted each other.

[1] During the Document Review Team's sessions with the Sequoia system, the Edge I unit was not in working condition. Since the firmware and documentation for the Edge I and Edge II are the same, we have little reason to believe that the results we report here would be different for the Edge I. Still, we note here that our hands-on experience with Sequoia DREs was limited to the Edge II.

[2] The Card Activator and one of the HAAT 50 units were inoperable during our walk-through sessions.

4.1.2 Election Creation and Ballot Management

Election definition in the Sequoia system begins with creating a new election in WinEDS.[3] An election definition was already installed on the WinEDS server, but we attempted to define our own election for the AVC Edge. The Optech Insight units and the 400-C were set up to read ballots for a different election than the one that was pre-defined in WinEDS. We followed the WinEDS documentation for creating a new election,[4] but were unable to complete this task. Our attempts to create a new election produced an error message about a failure to connect to the database that WinEDS depends on to store election definitions and data. Although the WinEDS Reference Guide states that "WinEDS creates a new election database and a new election log database, on your server,"[5] the Reference Guide—including the "Election Wizard Error Messages"—did not explain what this error means or how to resolve it.[6] Thus, for all Edge-related procedures, we used only the election that was pre-installed on the WinEDS server.

Similarly, we accepted the default ballot definition provided by WinEDS for this election. Based on our review of the WinEDS Reference Guide, defining different ballot styles appeared to be a time-consuming process with a large number of configuration options.[7] We concluded that our limited time to use the Sequoia system did not warrant an extended exploration of defining different ballot styles, though we note that this is an extremely important aspect of election management.[8]

4.1.3 Loading Ballot Definitions

The procedures for installing ballot definitions the AVC Edge, the Optech Insight, and the 400-C are all different. Ballot definitions and other election data for an AVC Edge are copied to a Results Cartridge using WinEDS. The Results Cartridge is then inserted in the Edge's Results Port. This step involves a number of security considerations, but we defer discussion of those issues to the Security section of this report.

[3] Sequoia Voting Systems, WinEDS (Windows Electronic Database System) Operators Manual Release 3.1 § 5, rev. 1.03, Jan. 2006 ("WinEDS Operators Manual"). Before using WinEDS to create or manage an election, the system must be installed and configured to define users, roles, etc. We discuss these aspects of WinEDS in the Security portion of this Usability section.

[4] WinEDS Operators Manual § 5.1.1.

[5] Sequoia Voting Systems, WinEDS Election Data System Reference Guide Software Release 3.1 at 4-3, rev. 6.02, Jan. 2006 ("WinEDS Reference Guide").

[6] *See* WinEDS Reference Guide at 9-9. The two Election Wizard Error Messages listed in the Reference Guide were not helpful in deciphering this error. *Id.*

[7] *See* WinEDS Reference Guide 5-49 - 5-75 ("Ballot Management Overview").

[8] *See, e.g.*, 2006 General Primary System Issues spreadsheet row 19, column E:

> County contracted with vendor to perform election definition/configuration programming for this election. On election eve, county discovered that WinEDS had been incorrectly programmed, such that it would correctly read/tabulate absentee ballots, but not regular ballots. Problem was corrected behind the scenes by: a) modifying program, b) performing new L&A to verify correct programming, and c) submitting updated tabulation program to SOS in accordance with EC [Elections Code].

From a usability perspective, we were able to follow the Sequoia system documentation—primarily the WinEDS Reference Guide, as the Operators Manual and the Voting Systems Use Procedures ("VSUP") for California[9] simply refer the reader to the Reference Guide—to create a Results Cartridge for the Edge. But the WinEDS interface presented, and the Reference Guide and other documents failed to clarify, a few questions.

First, one configuration option for a Results Cartridge is a choice between designating a serial number of the Edge unit that will use the cartridge, and simply selecting "None." The Reference Guide mentions this option but fails to explain any consequence of not associating a Result Cartridge with a specific machine; it simply states: The WinEDS Reference Guide simply states: "If you are creating an Edge cartridge, click the **None** check box to create a cartridge without a serial number and therefore specific to no one machine."[10] The Voting Systems Use Procedures (VSUP) contain a form for Results Cartridge serial number tracking,[11] but this does not clarify whether Results Cartridges *should* be programmed with specific Edge serial numbers. The Source Code Review Team informed us that the Edge will write its own serial number on a Results Cartridge that has no serial number specified.[12] Linking a Results Cartridge to a specific Edge unit could affect both the security and auditability of the voting system. The WinEDS Reference Guide or the VSUP should explain this choice and at least recommend a procedure.

After formatting a Results Cartridge, we proceeded to program the HAAT to activate vote activation cards.[13] The HAAT documents offered very little guidance about how to complete this task. Specifically, neither the HAAT Reference Manual nor the HAAT Pollworkers Manual describes how to prepare the HAAT to activate cards.[14] It was only by recalling the process from the Sequoia technician's demo that we were able to transfer HAAT files from the WinEDS server to the HAAT. This process involves burning HAAT files to the PCMCIA card, and then manually copying them to a USB drive to insert into the HAAT device. Thus, we found the document was basically insufficient with respect to HAAT usability.

4.1.4 Manual Vote Pre-Election Logic & Accuracy Testing (LAT)

The California Elections Code requires election jurisdictions to conduct "[n]o later than seven days prior to any election . . . a test or series of tests to ensure that every device used to tabulate ballots accurately records each vote."[15] Such testing is widely known as "logic and accuracy testing" ("LAT"). Accuracy testing refers to tests designed to determine whether equipment is in working order, while logic testing refers to tests designed to determine whether a voting system correctly interprets a voter's selections on a ballot.[16] In practice, these tests are lumped together to include touchscreen calibration and a few hardware checks performed while the

[9] Sequoia Voting Systems, Voting Systems Use Procedures for California (Optech Insight, AVC Edge 5.0 & Optech 400-C), rev. 1.05, Oct. 2006.

[10] WinEDS Reference Guide at 5-77 (emphasis in original).

[11] WinEDS Reference Guide at L-1 and M-9.

[12] We confirmed that an Edge unit will reject a Results Cartridge programmed for a different Edge.

[13] As noted above, the Card Activator was inoperable during our walk-through sessions.

[14] *See* HAAT Operations & Maintenance Manual § 4 (describing how to *use* a USB stick to prepare the HAAT, but not how the prepare the USB stick itself).

[15] Cal. Elec. Code § 15000.

[16] VSUP App. F.2 & F.3.

Edge is in maintenance mode, zero proof printing, and simulated or manual voting with the Edge in pre- or post-election mode.[17] The AVC Edge allows logic and accuracy testing before and after an election. We refer to these machine modes as pre-LAT and post-LAT, respectively.

The Sequoia AVC Edge allows two distinct types of pre-election LAT: manual vote and vote simulation. The VSUP do not specify whether to use one or both of these methods; this may be a jurisdiction-specific decision. Still, setting this question aside, we found the documentation basically insufficient for vote simulation and lacking self-containment for manual vote LAT.

The VSUP refer the reader to the AVC Edge Operators Manual for the details of both manual and simulated pre-LAT. The AVC Edge Logic & Accuracy Testing (LAT) Guide for Pre-Election and Post-Election ("LAT Guide") also contains instructions for pre-LAT and recommends performing a vote simulation, followed by at least one manual vote.[18] The AVC Edge Operators Manual, on the other hand, suggests the opposite order in § 4.1, but later, in § 4.3.3, suggests running the vote simulation first. The Guide does not state whether the order of these operations will affect the results.

In vote simulation pre-LAT, an elections staff member inserts voter activation cards but does not make selections on the test ballot. Instead, the Edge votes the ballots according to a script loaded on a Results Cartridge. (The Operators Manual clarifies that vote simulation is available only in pre-LAT and post-LAT modes and that the cartridge containing the vote simulation script is to be inserted into the Edge's auxiliary port.)[19] Before the simulation begins, the Edge displays a "Zero Proof Report," the purpose of which is to show that no votes have been recorded for the election defined on the simulation cartridge. At the end of the vote simulation script, the Edge displays the vote totals for the simulation, which should match the results known from programming the simulation with WinEDS.

In manual vote pre-LAT, a member of the elections staff marks his or her selections on the ballot. The AVC Edge documentation, however, is frequently unclear about how to make the transition from vote simulation pre-LAT to manual vote pre-LAT. Section 4 of the Operators Manual is internally inconsistent on the question of whether to perform manual vote LAT before or after the vote simulation. Beyond this, the Operators Manual shifts, in § 4, from describing vote simulation to manual vote pre-LAT to opening the polls for actual voting.[20] Section 5 then begins anew with loading the ballot from the Results Cartridge, running pre-LAT (with a suggested procedure that again reverses the order of manual vote LAT and vote simulation LAT), and opening and closing the polls.

The manual vote pre-LAT procedures suggested in these two sections differ in an important way from those found in the LAT Guide. Section 3.7 of the LAT Guide clearly instructs the person performing pre-LAT not to cast a ballot in manual vote LAT: "*Do not* cast the ballot" (emphasis in original). As a separate step, the LAT Guide instructs the pre-LAT tester to go backwards through the ballot, de-selecting all choices along the way, and to finish by pressing the Activate button. The LAT Guide also instructs the tester not to review a paper record of the manual vote LAT ballot.

We found this procedure confusing because section 5 of the Operators Manual offers a different procedure: "[R]ather than casting a ballot, press and hold the Activate button for 3

[17] VSUP App. F.6.

[18] LAT Guide §§ 3.5-3.6.

[19] AVC Edge Operators Manual § 4.3.3.

[20] AVC Edge Operators Manual §§ 4.3.3-4.3.5.

seconds to return to the Voter Inactive state." This statement makes pressing the Activate button sound optional when compared to the flat prohibition found in the LAT Guide.

None of these descriptions of manual vote pre-LAT states the consequence of casting a vote in pre-LAT mode. The AVC Edge did not present a warning against casting a vote in manual pre-LAT. During our walk-through with the AVC Edge, we performed manual pre-LAT by canceling as well as casting votes; neither pre-LAT procedure appeared to affect the official election results. We also reviewed a paper record of a manual pre-LAT ballot. The beginning of this record noted that that record corresponded to a pre-LAT vote.[21]

Finally, we followed two procedures for switching the AVC Edge from pre-LAT mode to Official Election mode: power-cycling the Edge and using the Technician Function.[22] The Technician Function procedure follows these steps: after switching the polls to closed, hold the Activate button for three seconds (at which time the Edge emits a beep), release the button, then press it again for three seconds. Neither of these pre-LAT switching procedures gave any indication or warning that we had cast pre-LAT ballots. Finally, the ballots that we tallied after testing the Edge in Official Election mode (see below) corresponded to the selections we had made. This result leaves the documents' warning against casting pre-LAT ballots a mystery. After closing the polls in pre-LAT mode and power cycling the Edge into Official Election mode, the Edge gave no indication that the Results Cartridge contained cast ballot records.

In summary, we found the documentation to be basically sufficient for manual vote pre-LAT, but the unexplained and somewhat contradictory procedures cut against the documentation's self-containment.

4.1.5 Vote Simulation LAT and Undocumented Cartridge Types

During our second walk-through session we attempted to perform vote simulation LAT, which requires a Vote Simulation Cartridge. As part of this effort, we also attempted to prepare and use Audit Trail Transfer and Technician cartridges. Our motivation to create and use the Audit Trail Transfer and Vote Simulation cartridges is that they play important roles in the Sequoia system's accuracy and reliability. The Vote Simulation cartridge allows a person with appropriate access to an Edge unit to conduct pre-LAT or post-LAT vote simulation.[23] This process, in turn, is portrayed in the documentation as a way of verifying that the Sequoia system accurately records and tallies ballots. The Audit Trail Transfer cartridge allows election officials to copy the contents of the Edge's Audit Trail Memory, in case a Results Cartridge is lost, damaged, or otherwise unreadable by WinEDS.[24] As the Edge Operators Manual notes, "*[t]he Audit Trail can only be transferred onto an Audit Trail Transfer Cartridge.*"[25] Finally,

[21] A possible explanation for the warnings against casting a ballot in pre-LAT is that doing so increments the protective counter. We were not able to confirm whether casting a vote in manual vote pre-LAT mode causes the protective counter to increment.

[22] In California, since pre-LAT must be finished at least seven days prior to an election covered by the Elections Code, the Results Cartridge door, the polls open switch, and the door covering the power switch are sealed. VSUP § 4.5 and App. F. These seals are supposed to remain intact until the Edge units are delivered to precincts and used for an official election.

[23] *See, e.g.*, AVC Edge Operators Manual § 4.1. The Vote Simulation and Results cartridges play a more prominent role.

[24] AVC Edge Operators Manual § 10.3.

[25] AVC Edge Operators Manual § 10.3 (emphasis in original).

we chose to try to use the Technician cartridge simply because it was largely undocumented.[26]

Our first finding with respect to these cartridges is that the documentation does not explain how to *create* them. Somewhat by accident we found that a drop-down menu on the WinEDS Results Cartridge creation widget that allowed us to choose to program non-Results cartridges. For all three types of alternative cartridges, we simply chose the cartridge type that we wished to create and then followed the remainder of the WinEDS Reference Guide's instructions for creating a Results Cartridge.[27] This process produced no warnings of any kind.

Our second finding, however, is that we were unable to use any of these cartridges. Moreover, neither the documentation nor the messages that the Edge displayed were helpful in diagnosing the problem. In the case of the Vote Simulation cartridge, we followed the Operators Manual's instructions for performing a pre-LAT vote simulation.[28] This procedure met an abrupt end after we inserted the Vote Simulation cartridge into the Edge's Auxiliary port, as directed. At this point the Edge displayed a message stating: "Error During The Simulation. Please Remove The Simulation Cartridge." We could not find any documents that explained the possible sources of error or how to resolve them.

For the Audit Trail Transfer Cartridge, after creating the cartridge, we followed the Operators Manual's instructions for transferring the Audit Trail: from the polls closed state, we switched to the Technician Functions screen[29] and selected "Audit Trail Transfer."[30] After being prompted, we inserted the transfer cartridge into the auxiliary port. The Edge rejected this cartridge as having been created for a different Edge unit. We reprogrammed the Audit Trail transfer cartridge several times and carefully checked the serial number on the programming screen, but ran into the same error each time.

Finally, the documentation does not state a use for the Technician Cartridge. We inserted it into the auxiliary port while the Edge was at the Technician Functions screen reachable from post-LAT mode. We attempted to return to post-LAT mode, but the Edge warned about an "invalid audio aux cartridge" and directed us to remove it from the auxiliary port. The Edge returned to post-LAT mode after we removed the cartridge.

Thus, we find that the Sequoia system documentation is basically insufficient with respect to creating Vote Simulation, Audit Trail Transfer, and Technician cartridges. The documents do not explain how to create any of these cartridges. Indeed, the documents do not explain the purpose of the Technician cartridge. Nor do the documents provide any help figuring out how to resolve the error messages that we encountered during our attempts to use these cartridges; the documents assume that these cartridges are on hand and that they will work without incident.

[26] The only documents in which we found of the Technician cartridge mentioned were the WinEDS Software Specification (see § 10.7.2.4) and the WinEDS AVC SDK (see App. B.1.1).

[27] *See* WinEDS Election Data System Reference Guide § 5-76 - 5-77 (rev. 6.00, software release 3.1), Dec. 2005.

[28] AVC Edge Operator's Manual § 4.3.3.

[29] This is done by pressing the Activate button in polls closed mode for three seconds, releasing it, and then pressing it again for three seconds.

[30] AVC Edge Operator's Manual § 10.3.

4.1.6 Election Day

Opening the Polls

We followed the steps in the AVC Edge Pollworker Manual (“Edge PWM”) to open the polls in Official Election Mode.[31] Though jurisdictions typically assemble and prepare their own pollworker manuals, our findings in this section are of interest to the extent that Sequoia’s pollworker materials form a basis for the materials that jurisdictions actually use. Examining jurisdictions-specific documents is beyond the scope of this report.

The Edge PWM contains separate instructions for issuing voter activation cards to regular and provisional voters.[32] The PWM also tells pollworkers not to activate voter cards in advance, but does not provide a reason. The principal difference between a regular and provisional activation card, as the PWM explains, is that a provisional voter’s activation card contains a unique number to identify that voter’s ballot, which the pollworker must read from the Card Activator display and copy to the provisional voter form. The Edge PWM does not explain the potential consequences of failing to record the provisional ballot identification number. Due to time constraints we did not walk through the provisional voting instructions.

Voting on the AVC Edge

We prepared vote activation cards and voted numerous ballots, including some with write-in selection. The contents of the AVC Edge Voter Instructions (Release 5.0) closely tracked the choices with which were presented by the Edge. We did not encounter any situations in which the documentation failed to explain what we needed to do as a voter. These documents are sufficient.

This situation was different for the materials pertaining to pollworkers. The AVC Edge documents list three conditions that require pollworker intervention: ejecting an invalid voter card, handling a ballot that a voter leaves without making any selections, and handling a ballot that a voter abandons after making at least one selection (a “fleeing” voter). We defer discussion of these situations to the Ballot Secrecy section below.

Voting on the Optech Insight

Overall, we had little trouble following the documents for voting, and administering at the polling place level, the Optech Insight. During our walk-through sessions we used pre-loaded ballot definitions; we did not attempt to create our own.

The Insight reads marks on paper ballots as defined by California Elections Code § 301(c). Voters mark their ballots in voting booths and then insert them into a secrecy sleeve. There is a discrepancy in between the PWG and VSUP about the next step in the voting process. The PWG directs pollworkers to have the voter detach the stub off the ballot and insert the ballot into the entry slot of the machine.[33] The VSUP direct the “precinct officer” to remove the stub and deposit the ballot into the ballot box (assume this means into the Insight) on the voter’s behalf.

[31] *See* Edge PWM § 5.

[32] Edge PWM § 8.

[33] PWG § 5.2(4).

Once complete ballot (one that contains no over- or undervotes, has no stray markings, and is not physically disfigured) is inserted into the machine, the Insight records the locations where it identifies marks onto a removable memory pack. If ballots are undervoted, overvoted, marred, disfigured or otherwise unprocessable, the machine will not accept the ballot. A message will be printed on the paper tape that feeds out the back of the machine and physically records significant events.[34] Neither the PWG nor the VSUP provides direction to pollworkers about (1) whether to rip off the printed error message or not; and, related but independent, (2) whether to read the error message to the voter or have the voter read it.

There are several options for handling a returned ballot. The voter may be issued a new ballot and the spoiled ballot so marked. If the voter believes the ballot to be error-free it may be fed again into the machine. Another possibility to is place the ballot in an auxiliary bin for later processing. Or, if the voter so chooses, the ballot can be resubmitted with a known-error through the use of the override button accessible to the pollworker on the back of the machine.

The method for handling a returned ballot affects whether the ballot is cast in the voter's presence. For ballots processed using the override option, the properly made vote selections on under- and overvoted ballots are recorded on the MemoryPack, and the vote counter is incremented. Undervoted and overvoted contests on such ballots are not recorded. Where "error"[35] or "unprocessable"[36] ballots are processed using the override option, the vote counter is incremented; but the voter's selections are not tabulated by the Insight at this time. A common reason for a ballot to be considered "unprocessable" by an Insight is if the "security Identification header code" on the ballots does not match the code expected by the Insight. This could be due to delivery of either an incorrect Insight or incorrect ballots to the polling place. In such instances, pollworkers are directed to contact election headquarters.[37] Where ballots are placed in the auxiliary bin, neither the fact that the ballot was cast nor the choices of the voter are captured by the Insight. At the end of voting hours, pollworkers are directed to remove the ballots from the auxiliary bin and insert them into the Insight for processing using the override key where necessary.

Closing the Polls

The California Elections Code provides a uniform poll closing time of 8:00pm,[38] though voters in line at that time must be allowed to vote (*id.* § 14401). Neither the poll closing procedures in the Voting System Use Procedures for California (VSUP) (§ 5.7.2 and App. I.2) nor the procedures in the AVC Edge Operators Manual (§ 4.3.9) mention this official declaration, though the VSUP procedures for the Optech Insight do.

AVC Edge For detailed poll-closing procedures, the VSUP refers the reader to the Operators Manual. The Manual, in turn, instructs pollworkers to:

1. Break the seal on the polls switch cover and switch the Edge unit to polls closed mode.

[34] These events are also recorded in MemoryPack.

[35] VSUP p. H-5

[36] VSUP at H-5

[37] Optech PWG § 5.3.2.2

[38] Cal. Elec. Code § 14212.

The Operators Manual does not instruct the pollworker to record the seal number or take any steps to preserve it.

2. Wait for the results report to print, tear it off, and sign it.

3. Break the seal on the Result Cartridge door, remove the cartridge, and place it in the Cartridge envelope.

To be part of a chain-of-custody that provides evidence of tampering, security seal numbers must be tracked throughout their use on a piece of equipment, and records of this tracking must be available for auditing. Thus, the documents provided by Sequoia are insufficient for the purpose of maintaining the proper chain-of-custody.

The Office of Voting Systems Technology Assessment memorandum on Sequoia use procedures ("OVSTA Memo") requires pollworkers to take additional steps to document how seals are handled. For example, the OVSTA Memo requires election staff to maintain logs of the memory cartridge serial numbers assigned to each Edge machine, as well as the serial number of each Results Cartridge door seal. The OVSTA Memo further requires election staff to inspect the seals prior to the opening of the polls, and the Memo sets forth procedures for documenting and taking action in response to broken seals under a variety of circumstances. These elements of logging, inspection, and reconciliation of security seals are missing from the Sequoia documents.

In addition, California requires each precinct to post "a copy of the result of the votes cast at the polling place" on election night.[39] Each Edge unit provides a Results Report after it is switched to polls closed mode. Neither the Operators Manual nor the VSUP relate the poll closing to the vote totals posting requirement of California law; the VSUP simply refer the reader to the Operator's Manual, which are not specific to California.

Optech Insight After the polls are closed, pollworkers use a key to unlock the rear access lid of the Insight, and using the keypad, print the Ballot Report[40] and the Vote Totals Report[41] for the machine. Pollworkers are directed to tear off the Vote Totals Tape (it is unclear from the documentation whether pollworkers should tear off or leave intact the rest of the tape, including the Ballot Report and event logs) and, if directed by the jurisdiction, sign it.

Pollworkers are then directed to power off the Insight and, if directed by the jurisdiction, break the seal on the memory pack door and remove the memory pack. Some jurisdictions require the memory pack to remain in the machine, which, as discussed below, is a positive mitigation measure. The PWG and VSUP direct pollworkers to record the number of the broken seal in the pollworker log sheet.

The PWG and VSUP sections about poll closing procedures fail to direct the pollworker to record the date and time the seal is broken and the name of the individual (pollworker, in this

[39] Cal. Elec. Code § 19384.

[40] The Ballot report contains statistics determined during the election set up.

[41] The Vote Totals report contains the vote totals for each candidate and proposition on ballots read by the Insight.

instance) who breaks it as required under the Security section of the VSUP § 10.[42] Nor do the documents in the relevant sections about procedures during poll closing direct the pollworkers on what to do with the destroyed seals.[43] For these reasons, the documents pertaining to the Optech Insight are basically insufficient for poll closing procedures.

In jurisdictions that direct pollworkers to remove the MemoryPack, the PWG and VSUP direct pollworkers to place it in a provided anti-static bag and return the bag to the election office. The pollworker then removes the Insight from the top of the ballot box and removes the ballots from the exception and regular ballot bins, bundles them separately, and returns them to the election board. PWG §7. Section 8.9.1 of the VSUP erroneously directs the "operator" to insert a floppy diskette into the Insight to make a backup copy of the vote totals. The Insight has no floppy disk drive, making this impossible.

Tallying Results

The documentation for tallying results from the Optech Insight was clear. We encountered no difficulties in reading a MemoryPack that had stored after scanning our test ballots.

However, we had some difficulty tallying ballots from the AVC Edge cartridge. When we attempted to tally results, WinEDS displayed an error message stating that results from that machine had already been tallied. We determined that this was likely an artifact of the test environment; we used the same Edge to run through multiple "Election Days." Still, resolving the error by use by referring to the documentation took a significant amount of searching.

4.2 Security

Perhaps no aspect of electronic voting has attracted more attention than security. The Top-to-Bottom Review presents an opportunity to review the security requirements of California law as well the VSS, and to examine voting system documentation in light of those requirements. We emphasize, however, that we have drawn no conclusions as to the sufficiency of Sequoia's documentation under any of these standards. Instead, we sought to determine whether the available documents (1) present security issues in sufficient detail to allow an election official to understand them and (2) provide sufficient detail about security tests to allow the reader to understand how those tests were performed.

For background, we summarize the security requirements of the VSS and California elections law and regulations and discuss how the centrally important ITA and state testing reports document security testing of the Sequoia system. Next, we discuss security issues common to the optical scan equipment, AVC Edge, and WinEDS in documents such as ITA report and the VSUP. Finally, we discuss issues specific to each of these components.

[42] VSUP § 10.1.6 provides: "audit logs must be maintained recording the sealing, including the seal number, the date and time, and the person's name, as well as the unsealing, including the seal number, the date and time, and the person's name."

[43] According to the Sequoia Voting Systems Optech Insight Plus Operators Manual, rev. 1.01, Sept. 2005, Part number 190-32827-00, §8.1, broken seals should be placed "in the plastic bag marked Seals and return[ed] . . . to the Election Board."

4.2.1 VSS

The VSS approach voting system security from three angles. First, in Section 6 of Volume I, the Standards set forth security performance requirements, including access control policies, individual access privileges, physical security measures, and software security measures.[44] A section of the VSS is devoted to security standards, which include such measures as access controls, physical security measures, software security (including restrictions on the placement of certain types of software within the voting system), and network security.[45] The VSS also provides minimum requirements for audit records.[46] Second, the VSS require vendors to submit documentation that describes how the vendor took security into account in the design and development of its voting system. For example, the vendor must provide the "plans, procedures, and data used during software development and system integration to verify . . . security."[47] Vendors also have the option of including recommended security procedures with the submissions to ITAs.[48] Such documents do not, however, provide much help to a reader of an ITA report who wishes to understand the procedures and conditions used to test voting system security. Finally, the VSS require the ITA to "design and perform test procedures that test the security capabilities of the voting system against the requirements defined in Volume I, Section 6."[49]

4.2.2 ITA Reports

The ITA test reports for the Optech Insight, 400-C, AVC Edge, and WinEDS are uniformly unhelpful in establishing an understanding of the tests conducted to assess voting system security.[50] Most significantly, the software qualification test report for WinEDS does not contain the VSS requirements matrix that the other reports use to document that they tested all applicable requirements of the VSS. This is a basic, and serious, insufficiency in the documentation.

Overall, the ITA reports display a lack of self-containment. For example, they do not state whether the source code review of firmware occurs before security tests; nor do they state whether hardware testers are made aware of the results of a source code review. The VSS specifies a "general" sequence—hardware functional and performance testing, source code review, software functional and performance testing, and finally functional and performance testing of the integrated system.[51] The ITA reports do not state whether the ITA adhered to (or

[44] The VSS approach to security has been criticized for taking an excessively functional approach to security and neglecting more open-ended testing. *See, e.g.*, ACCURATE, Public Comment on the 2005 Voluntary Voting System Guidelines, http://accurate-voting.org/accurate/docs/2005_vvsg_comment.pdf, Sept. 2005 (criticizing the 2002 VSS).

[45] VSS Vol. I §§ 6.2-6.4. *See also* VSS § 4.2.2 (restricting the use of "[s]elf-modifying, dynamically loaded, or interpreted code").

[46] VSS Vol. I § 4.4.2.

[47] VSS Vol. II § 2.7.1.

[48] VSS Vol. II § 2.8.7.

[49] VSS Vol. II § 6.4.

[50] Ciber, Inc. served as the ITA for WinEDS, while Wyle was the ITA for all Optech and all Edge components except the HAAT (which was evaluated by Systest).

[51] VSS Vol. II § 1.4. *See also* Carolyn Coggins, *Independent Testing of Voting Systems*, 47 COMM. ACM 34 (Oct. 2004).

departed from) this sequence, nor do they contain the test plans that the ITA actually used.[52] One element of Sequoia's technical data packages was a test and verification specification for the Optech, Edge, and WinEDS.[53] Aside from referencing these specifications, the ITA reports do not state whether or how the ITAs applied the security-related specifications. We provide further details about these specifications in the component-specific subsections below.

In summary, some of the Sequoia ITA reports, standing alone, do not tell the reader which security-relevant requirements for the VSS were tested for each major system component. Moreover, the reports do not reveal the methods for testing each of these requirements; nor do they provide the reasoning that supports the ITA's conclusions. An exception to this rule is the HAAT test report from Systest, which provides space for the tester's comments next to each requirement in the functional testing matrix.

4.2.3 California

The California Elections Code has little to say about voting system security. However, documents concerning voting system security in general, and Sequoia system security in particular, have been issued by the Office of the Secretary of State. For the Sequoia system, two such documents are particularly important. The first is the official certification of the Sequoia system, which made the system's certification conditional on Sequoia's providing use procedures that cover such topics as attaching serial numbers to removable media, using tamper-evident seals, and documenting the chain of custody for each Optech memory pack and Edge memory cartridge.[54]

California's Office of Voting Systems Technology Assessment Secretary of State has also issued a memorandum ("OVSTA Memo") setting forth requirements that overlap with the Sequoia certifications requirements for tagging, sealing, and logging removable media for the Edge and Optech Insight.[55] Like the Sequoia Certification, the OVSTA Memo directs pollworkers to verify security seal serial numbers on Edge and Optech Insight units, to examine their integrity, and to investigate any breaches of the seals or the chain of custody. In addition, the OVSTA Memo requires jurisdictions to program memory packs and memory cartridges in a secure facility. This requirement is not found elsewhere in the Sequoia documentation. We discuss its significance in the subsections devoted to the Optech Insight, 400-C and the AVC Edge, below.

Finally, prior to the Secretary of State's certification of the Sequoia system, OVSTA tested the system and published its analysis ("Sequoia Staff Report").[56] The Sequoia Staff Report adds little information about the Sequoia system's security to the findings in the ITA reports. This report's test plan does not describe anything specific to security testing;[57] its only evalua-

[52] *See* VSS Vol. II § 1.4 (noting that the ITA "[d]evelop[s] . . . a detailed system test plan that reflects the scope and

complexity of the system, and the status of system qualification").

[53] *See* VSS Vol I § 7.7.c.6 (stating that a "system test and verification specification" as part of the "minimum" set of documentation requirements).

[54] *See* Approval of Use of Sequoia Voting Systems, Inc. DRE & Optical Scan Voting Systems ¶ 4.f, March 20, 2006.

[55] *See* OVSTA Memo.

[56] *See generally* OVSTA, Staff Review and Analysis, Feb. 22, 2006 ("Sequoia Staff Report").

[57] *See* Sequoia Staff Report at 27-31.

tion of the Sequoia system's security is that "with procedures in place, the proposed system is at least as effective in maintaining the . . . security of the elections process . . . as the currently certified Hart system."[58] The Report does not explain how OVSTA staff arrived at this conclusion, or why a comparison to a currently certified system rather than the 2002 VSS or state requirements is appropriate.[59] Also attached to the Sequoia Staff Report was a Consultant's Report,[60] which finds that the Sequoia system maintains an "appropriate" level of security, so long as the "appropriate" operating procedures are in place.[61] The Consultant's Report does not state what those procedures should be.

4.2.4 WinEDS

A central component of maintaining security and integrity of election results in the WinEDS system is access control. The documentation states that "the purpose of WinEDS security is to allow users of WinEDS to accomplish the tasks they have the rights to do, on the workstations they are authorized to use."[62] Access control in WinEDS also provides a means to (1) prevent unauthorized users from using WinEDS; (2) limit uses to those that are authorized for a particular user; and (3) limit the use of a workstation to a list of authorized users or a set of authorized tasks.[63]

In addition to providing security, access control also provides a means of protecting the election system from potential errors and mistakes that may arise when users accidentally perform certain actions that may affect the integrity of the election data. Users should only be given as much permission as they need to perform the task they are assigned.

Access control is also important for auditing purposes. The documentation states that the jurisdiction should "monitor role and user permission[s] to detect unauthorized access."[64] In addition to unauthorized access concerns, audit trails can assist election officials in debugging problems with election results issues that may arise from misconfiguration issues or accidental activation of some features.

One method of providing access control is through physical security: restricting who can access the WinEDS computer. This can be achieved by housing the WinEDS machine in a secure facility and limiting access to only the personnel who are authorized to use the WinEDS system. The documentation recommends that the using jurisdiction should implement physical security measures to keep the WinEDS system in a locked secure room with a security monitoring system, as well as limit system users to authorized election personnel.[65]

WinEDS has a system for providing controls over users' roles, workstation-based access control and user-based access control. In WinEDS, roles are the central mechanism for enforcing security policies. In short, roles are assigned components, which are assigned attributes.

[58] Sequoia Staff Report at 24.

[59] *See* Cal. Elec. Code §§ 19250(a), 19251(d) (requiring that a voting system containing a DRE to be federally qualified).

[60] Paul Craft, California Secretary of State Consultant's Report on Sequoia Voting Systems, Inc. WinEDS/AVC Edge/Insight/400C/Eagle/HAAT, Feb. 24, 2006 ("Consultant's Report").

[61] Consultant's Report at 2.

[62] Sequoia Voting Systems WinEDS Security Specification Release 3.1, rev. 1.04, Jan. 2006, at 2-1.

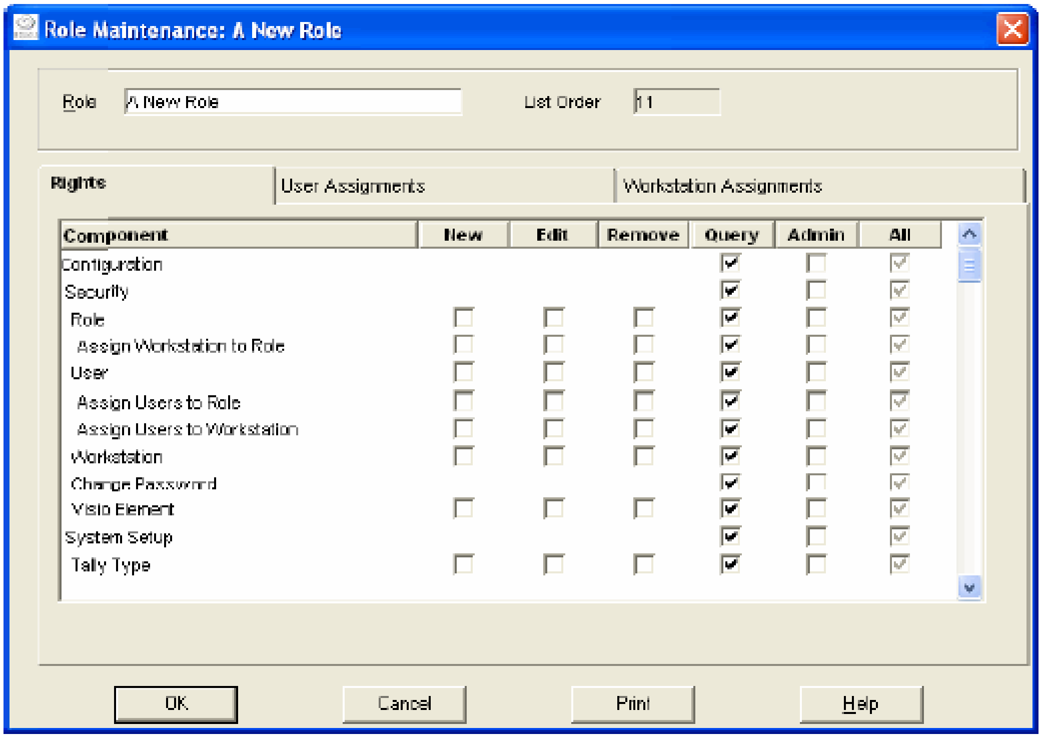
[63] *Id.*

[64] *Id.* at 6-2.

[65] *Id.* at 2-3.

These roles are then applied to users or workstations. The users or workstations then take on the capabilities of their assigned roles. Users log into workstations, and in the case where a workstation and a user both have defined roles, the actual rights that are executed are only the rights that both have in common.

Roles are created by an administrator, and assigned capabilities, or as they are referred to in the documentation and user interface "components". Components are capabilities such as "Assign Users to Role" or "Tally". Each component has up to six potential attributes. The attributes per component are new, edit, remove, query, admin or all. Each one of these attributes can be selected by clicking on a check box in the role assignment UI [Figure 4.1]. The administrator can select any combination of attributes based on what they would like to assign to that component. For example, an administrator may decided to assign the "Assign Users to Workstation" component with new, query and edit, but not remove and admin. All checkboxes for that component can be selected by clicking "all". In total, there are 111 components, or capabilities, that each role can be assigned. The total number of checkboxes is 615 checkboxes, of which 72 (12 rows of 6 columns) are visible in 4.1.



Role: A New Role

List Order: 11

Component	New	Edit	Remove	Query	Admin	All
Configuration				☑	□	☑
Security				☑	□	☑
Role	□	□	□	☑	□	☑
Assign Workstation to Role	□	□	□	☑	□	☑
User	□	□	□	☑	□	☑
Assign Users to Role	□	□	□	☑	□	☑
Assign Users to Workstation	□	□	□	☑	□	☑
Workstation	□	□	□	☑	□	☑
Change Password				☑	□	☑
Visio Element	□	□	□	☑	□	☑
System Setup				☑	□	☑
Tally Type	□	□	□	☑	□	☑

Figure 4.1: Role Assignment User Interface

The documentation states that users should be assigned specific roles.[66] The WinEDS application comes preconfigured with 10 roles, and the administrator may choose to create new roles or modify these in the interface described above. The preconfigured roles are listed in Table 1 below.

The most important of these predefined roles is the Administrator role. The Administrator

[66] *Id.* at 2-2.

Table 4.1: Predefined Roles in WinEDS

Administrator
Clerk
Technician
Tally Worker
PHASE I-Election Data
PHASE II – Ballots
PHASE III - Machine Programming
PHASE IV – Tally
PHASE V - Post Election
PHASE VI - Archived

role typically runs as the most powerful role in the system, the System Administrator (sa). The sa role comes predefined with all 615 checkboxes selected. The other roles come with various subsets of boxes selected. The sa role can perform all functions in WinEDS, as well as define additional roles and create users or workstations. Because of the power of any administrative account, WinEDS recommends that users "[a]void logging into the application as the System Administrator (sa). Each user should always login using their user log in."[67] This is especially apparent in the case of running the tally of votes on election day. It states in the documentation that "it is always a good idea to have a role for Tally only and have several users that are assigned for this role. This will keep random or mistaken mouse clicks from stopping tally or pull reports are [sic] inappropriate times."[68]

The Tally is an important part of the election process and comes at a time when the system is particularly vulnerable to mistakes and data corruption, as well as potential malicious attacks. For these reasons, the documentation recommends additional security measures be taken during the Tally phase. The documentation stresses additional physical security for tally machines, such as never leaving tally machines unattended at a remote tally site, and ensuring that tally workstations that have "input/output devices such as floppy disk drive or CD-ROMs" be "protected and locked to prevent unauthorized uploads and downloads."[69] Additional documentation states the importance of having separate tally accounts. In the case of jurisdictions who may employ seasonal workers, the documentation recommends that the jurisdiction "determine policy for access to temporary or seasonal employees via disable account option" and recommends "setting seasonal employees to inactive in non election periods."[70]

The importance of the Tally phase in terms of access control makes it a good candidate to observe the usability of pre-configured access components. In addition, there existed some ambiguity in the documentation about what the Tally role could actually perform without a degree of administrative access. The documentation states[71] that three capabilities of the sa user are required to tally the election, notably starting the tally, stopping the tally and resetting

[67] Sequoia Voting Systems WinEDS Security Specification Release 3.1 Doc Ver 1.04 January 2006 pg 6-2

[68] WinEDS I System Training Pre-Lat and Tally Training Manual pg 91

[69] Sequoia Voting Systems WinEDS Security Specification Release 3.1 Doc Ver 1.04 January 2006 pg 2-3

[70] WinEDS 3.1 Reference Guide Release 6.02 January 2006 A-6

[71] WinEDS 3.1 Reference Guide Release 6.02 January 2006 6-3.

the data store.[72] In addition, the documentation states that "although the user will have to enter the sa password to perform the above mentioned [tally related] tasks, this is still a good check and safeguard."[73] However, the documentation also describes as stated above that there should only be a specific role for the Tally only. As stated in the documentation, it seemed good security practice to have a differentiation of roles per function.

To test this, we configured a single WinEDS machine to run an election and tally the results. It was not stated in the documentation or help what the difference was between the pre-defined Tally role as well as the Phase IV Tally role, so we decided to try them both. After launching WinEDS, we logged in as sa, created a new user, and assigned the role Tally to our new user. We then logged off and logged back in as the new user Tally. In our first test, we were unable to run anything as the Tally user. All menu items were grayed out, and we were unable to perform any actions on WinEDS. We decided to close WinEDS, and open it as the sa user again. This time, we cleared the database of previous tally results, started the tally, and then logged out as the sa user. We then logged back in as the Tally user, and again were unable to perform any operations.

For our next test, we decided to remove the Tally role from our new user, and assign the Phase IV Tally role to our user. We performed the previous steps of clearing the database, and then logging in as the Phase IV Tally user. In this instance, we were able to tally the election. However, in examining the components and attributes assigned to each role, we found a significant difference between the two. The Tally role consisted of only components related to the tally. In contrast, the Phase IV Tally role consisted of many components and attributes, many of them with administrative privileges. These privileges allow a Phase IV Tally user to perform the additional functions in including all security functions in addition to tallying the election. After logging in as a Phase IV Tally user, we could change our access permissions to administrator—thereby allowing us to perform any operations in WinEDS as the Phase IV Tally user. This defeats any attempt at regulating the functions of the tally phase.

It is important to note that this was not a rigorous scientific analysis of this process, and there may be many additional factors that we were unaware of that lead to this outcome. It was our intention to better understand the documentation by using it to run through scenarios that an election official may have to perform.

With this caveat, the results of our tests do raise an important point. It is unclear that the access control mechanism for Tally mode could function without some administrative privileges or access as stated in the documentation. Namely, if the access control mechanisms do not function as users expect or are too complicated for end users to configure properly, users might leave the WinEDS machine logged in as the sa user. This action would run counter to the best practices stated in the documentation. It would also force a heavier reliance on physical security measures to ensure application security. Additionally, leaving the application logged in as the sa user makes the system more vulnerable to misconfigurations as a result of user action. As described in the documentation, "mistaken mouse clicks" or users navigating the interface and activating features in an attempt to accomplish their tasks while logged in as sa, could result in errors (including data integrity errors) that would require significant time to find and fix.

[72] WinEDS I System Training Pre-Lat and Tally Training Manual at 91.

[73] WinEDS I System Training Pre-Lat and Tally Training Manual 91.

In summary, we find the documentation relating to WinEDS security to lack self-containment. The documents raise some awareness of the security issues involved in configuring WinEDS, but the practical guidance in the available documents falls far short of what appears likely to help election officials configure WinEDS to mitigate against accidental or malicious altering of election data.

4.2.5 Optech Insight

This section considers the sufficiency of information about security threats (and mitigations) found in the documentation for the Optech Insight. The documentation is basically insufficient with respect to information about the kinds of threats that the Insight's use of cryptography are likely to withstand. But the documentation gives a considerable amount of information about access control, physical security, and maintaining a chain-of-custody. We discuss these two aspects of the Insight security documentation in turn.

Cryptography Ballot definitions and precinct header information for the Optech Insight are programmed onto MemoryPacks by election officials using WinEDS. These data are not encrypted on the MemoryPacks. Nor are ballot images encrypted while in storage on the MemoryPacks. Instead, checksums are used to verify that the ballot definition files and precinct headers placed on the MemoryPack are not tampered with prior to installation on the machines.[74] However, checksums are a relatively lightweight mechanism for assuring the integrity of information and, as used in the Optech Insight, are easily spoofed.[75] While the Insight's use of checksums might provide some check against unintentional corruption of files or data, they provide little protection against actual malicious activity.

Furthermore, the OVSTA staff report for the Sequoia system does not indicate any examination or testing of the Insight's data protection measures, nor does it contain a review of policies and procedures related to system security.[76] In particular, there is no discussion of the limitations in the Insight's use of cryptography. The documents are basically insufficient in this regard.

Access Control The documentation of access control (physical and technical) for the Insight, on the other hand, provides some practical guidance but, again, does not point out any of the limitations of the access controls for the Insight. The principal documents on this point are the OVSTA Memo, state certification, and the Insight Security Specification.

The Insight's design and the context in which the machines are used are important considerations in the documents. The Insight and Insight Plus are relatively unsophisticated machines. They have no capacity for password protection, although a PIN can be set to provide some marginal limitations on system use. The Insight and Insight Plus are used in the precinct and

[74] *See* Optech Insight Security Specification §§ 2.2, 3.6, rev. 1.01, Sept. 2005 (discussing the use of "checksum security" on MemoryPacks.)

[75] Further details about the weaknesses of the Insight's use of checksums to protect the integrity of data are given in the Sequoia Source Code Review Team's report.

[76] *See generally* Secretary of State Office of Voting Systems Technology Assessment, Staff Review and Analysis of Sequoia Voting Systems, Inc., Feb. 22, 2006.

therefore are used and accessed by pollworkers and voters in addition to election administration officials and employees.

The documentation supplies a number of procedures and measures to lend some security in this overall context. The Certification requires MemoryPacks to have permanent serial numbers assigned and affixed, and it requires jurisdictions to log and track these numbers. The Certification also requires MemoryPacks to be programmed in a secure facility under the supervision of the registrar of voters. Furthermore, MemoryPacks must be inserted into assigned machines and sealed with a serialized tamper-evident seal, which also must be tracked.[77] The machines must be delivered to the polling place with the MemoryPacks installed and protected with a tamper-evident seal and behind a locking door.[78] If any seal is broken on an Insight, the machine must undergo a full manual reconciliation with the MemoryPack record.

The seals currently in use in California, however, are not particularly robust. They can be easily broken and reassembled or replaced with copies that are readily available. The documentation does not address this point. In addition, the documents do not specify how to transport MemoryPacks *after* an election. Some jurisdictions leave MemoryPacks in the Insight units. This may provide some additional protection against tampering. In other jurisdictions, however, MemoryPacks are removed by the pollworkers after the polls are closed and the relevant reports are printed. In such instances a physical barrier to tampering is removed, leaving the MemoryPack vulnerable to a range of attacks as described in the Source Code Review Team's and Red Team's reports. The documents do not discuss the differences between these two procedures.

The Security Specifications for the Insight and Insight Plus provide some direction on roles related to security and segregation of duties. For example the documentation states that the election administration official is intended to have control of the key to the "rear access lid lock," which allows access to the circuitry of the machine; the maintenance technician can use a four-digit pin to run internal diagnostics on the machine and has full access to the machines keys; pollworkers do not need the four-digit pin for their job responsibilities and should therefore not have it. Given the information and access provided to the maintenance technicians they should *never* serve as pollworkers.[79]

The Security Specification provides detailed direction with respect to the information to be captured in the tamper-evident seal audit logs, and what events should be logged.[80] The Security Specification also documents the event logs created by the system. Given the limited options for protecting the security of the Insight and Insight Plus systems through anything but physical means, the Security Specifications provide useful guidance to election administrators on roles, segregation of duties, physical control mechanisms, and audit tools designed to limit and identify misuse of the machines. The Optech Insight Personnel and Training documentation provides useful information about the skills necessary for various roles but provides no discussion of the security implications of the roles. The roles described, while useful, are not

[77] OVSTA Memo ¶ 2.

[78] *See id.*

[79] Optech Insight Plus Security Specification September 2005, Part Number190-32825-00, p. 3-1 (the Insight documentation is identical in all material respects necessary for this analysis and will therefore not be separately cited.). *See also id.* §§ 5.4-5.5 documenting the discrete roles of pollworkers and maintenance technicians, although neither is defined in the glossary.

[80] *Id.* at §3.2.

uniformly referenced in other system documents.[81]

4.2.6 Optech 400-C

The documentation discusses physical and software-based security measures for the 400-C. With respect to access control measures for the 400-C the Security Specification recommends physical security measures, such as keeping the 400-C in a locked room with limited access, and hardware security features such as locks on doors and panels.

With respect to software controls the Security Specification states that, "Windows passwords may be used to protect against unauthorized entry into the system" and states that "secure desktop products are available . . . which provide restricted access to applications and the operating system, plus logging of intrusion attempts."[82] It also recommends First Security Agent, a third-party software program that provides a way to specify and enforce user-level security.[83] The implication, confirmed by our examination, is that the 400-C is by default configured with one account—an Administrator account—that runs with no password. Thus, as the machine is received by counties, its sole prophylactic protections against intentional misuse of the system are physical.[84]

The Security Specification and other documentation provided with the 400-C do not outline individual access controls in a manner that appears to be helpful to jurisdictions developing security measures.[85] There is no discussion of using roles to improve security. Also, the limited references to password management are confusing. In one place the documents direct counties to develop procedures for individual passwords that are complex and frequently changed, while in another instance, the standard for a password is a "minimum of 6 characters, 8 preferred."[86]

The VSUP provide more specific direction about security procedures.[87] For example, the VSUP direct election officials to verify and submit a statement to the Secretary of State that no program has been installed or resides on the Optech 400-C that is designed to work with Direct Access Objects,[88] and that the Optech 400-C should not be left unattended without first activating one or more levels of password protection.[89] Overall the VSUP for the 400-C provide more guidance and direction to local election officials. Given the lack of strong technical mechanisms to limit misuse of the system, there is little built-in protection against insider misuse of the 400-C. The use of add-on software to enable role based access and the frequent examination of audit logs are important steps documented in the California procedures. Maintaining

[81] Optech Insight Personnel and Training Requirements v. 1, Sept. 2005 Part Number 190-32609-00

[82] Optech 400-C Security Specification March 2004, Part Number 190-32374-00, p. 1-1, 2-1, 4-1.

[83] *Id.* at 6-1.

[84] In addition, despite the fact that the VSS, the Security Specification, and the California Voting System and Use Procedures all direct that unauthorized software should not be run on the system the system delivered for our study contained Google Desktop Search, Internet Explorer, Windows Movie Maker, MSN Gaming Zone, NetMeeting, and Outlook Express, Minesweeper and 3-D Pinball.

[85] The 400-C Maintenance Manual specifies what training is appropriate for Sequoia technicians, for example, but does not specify what roles they should (or should not) play in actual elections. *See* Sequoia 400-C Ballot Counter System Maintenance Manual §§ 6.6.1-6.6.4, rev. 1.01, July 2003.

[86] Optech 400-C Security Specification p. 5-1.

[87] *See* VSUP § 10.

[88] VSUP § 10.1.3.

[89] *Id.* § 10.2.2.1.

strong physical security over these machines is also critical.

4.2.7 AVC Edge

The documentation for the AVC Edge displays many of the deficits that are present in the WinEDS, Optech Insight, and 400-C documentation. The hardware qualification report, for example lacks details about how its hardware and (especially) its firmware were tested. This report also omits the grounds for the ITA's conclusion that the Edge meets the applicable VSS standards. Similarly, the OVSTA Staff Report and Consultant's Report—which do not make component-specific security findings in the first place—do not state how those evaluators tested security.

Other documents that specifically discuss the security of the Edge exhibit a pattern of discussing technical security measures or security-enhancing procedures without giving much information about the relevant threat or threats. As we illustrate below, this approach to documenting security fails to provide election officials with background that might help them evaluate the Sequoia system's security for either certification or purchasing decisions. Similarly, this approach omits information that might be helpful in election officials' or pollworkers' understanding the importance of recommended or mandatory security procedures.

Before discussing the overall lack of context in the Edge's security-related documentation, it is helpful to review the technical and procedural security measures that Sequoia and the state have documented. Though the AVC Edge Security Overview states that "[s]ecurity and integrity were cornerstones of the design philosophy of the AVC Edge,"[90] the Edge Security Overview fails to describe how the Edge's design incorporates security. Instead, the Overview describes certain characteristics of the Edge and argues that they enhance security.

The principal features asserted by the Overview are:

- The Edge does not have "any black-box COTS modules or components."[91] The available documentation does not discuss whether this customization is *ipso facto* more secure than a design that involves COTS components, or whether it is more secure than certain COTS components. The context for understanding this statement is missing in the Security Overview and throughout the Sequoia system documentation.

- "[M]alicious software" *cannot* be introduced into the Edge.[92] The Overview cites administrative controls in its software development process, manufacturing, and distribution of equipment to its customers as means to thwart attacks on the Edge's firmware. Other documents for the Sequoia system set forth ways in which physical security, the use of tamper-evident seals, and maintaining a strict chain of custody might protect against such tampering. These descriptions, however, do not answer the question of whether the Edge was developed to resist threats in the event that physical security measures fail.[93]

[90] AVC Edge Security Overview Release 5.0, May 10, 2005, at 3.

[91] AVC Edge Security Overview at 4.

[92] *Id.* at 8.

[93] *Id.* at 8. The Overview notes that the system's qualification under the FEC's 2002 VSS confirms that the Edge's "firmware is written in a high level language and is well designed." This statement provides no further clues about how this design enhances security, or how Sequoia or an ITA tested this design for security.

- The Edge has no capacity for networking and, on this basis, the documents assert that "[e]rrors cannot be promulgated from one machine to another."[94] This statement entails an assumption that a network is the only way to propagate an attack. The documentation provides no further detail about what kinds of threats might be present if the Edges were networked, or, conversely, how attacks might propagate through means other than a network. The Sequoia Red Team has identified at least two attacks on the Edge that involve spreading malicious software via memory cartridges.[95] The documentation's focus on one specific means of spreading malicious software—networks—would make it difficult to evaluate the security of the Edge against attacks that could spread from machine to machine through other means, such as memory cartridges.

- According to the Security Overview, the Edge will refuse to load data (e.g., ballot definitions) from a Results Cartridge that carries a serial number different from the Edge's serial number. This statement is consistent with the WinEDS Reference Guide's description of how to create a Results Cartridge, but it leaves an important gap: there is no explanation of the consequences of creating a Results Cartridge that does not contain a destination machine's serial number. In fact, as we discuss in the Usability section, none of the Sequoia documents, including the VSUP and the OVSTA Memo, tell the reader whether it is preferable to create a machine-specific Results Cartridge, or the reasons that that is so. This gap is especially perplexing given the Security Overview's assurance that, when tallying results from AVC Edges, WinEDS checks each results cartridge to verify that the machine serial number on a cartridge matches the number of a machine that was used in the election.[96]

- The Edge verifies ballot data on a memory cartridge by calculating the cyclic redundancy check (CRC) value and comparing it to the WinEDS-generated value on the cartridge.[97] Again, a threat model is missing from this description: the Security Overview does not state what technical measures, if any, would prevent an attacker with access to WinEDS or the memory cartridge from spoofing those values.

- The Security Overview's descriptions of ballot image and vote tally data storage security are difficult to follow and lack information sufficient to understand against what kinds of threats these measures help to protect. For example, the Security Overview states that the Edge appends a CRC value to each ballot record and performs a bit-level comparison of each record on the results cartridge with the corresponding Audit Trail record.[98] Again, the available documentation does not present these integrity-checking measures in the context of a potential attack against the AVC Edge, and leaves unanswered the question of whether an attacker could simply replace ballot records and their CRC values.

[94] *Id.* at 8; *accord* VSUP § 10.2.1, which states under the "For AVC Edge" heading: "The Optech Insight precludes the possibility of any non-essential services and ports." We interpret this statement to apply to the AVC Edge.

[95] *See* Sequoia Red Team Report.

[96] WinEDS maintains a database of each Edge's serial number used in an election.

[97] AVC Edge Security Overview at 5.

[98] AVC Edge Security Overview at 6. This part of the Security Overview also states that the Edge chooses random blocks of memory to store ballot records in order to mitigate against threats to ballot secrecy. *Id.* We discuss this further in the Ballot Secrecy section of this report.

- The Edge calculates cryptographic signatures for various totals files and stores these signatures on the results cartridge and in the Audit Trail memory.[99] The available documents, however, do not state how the Edge (and WinEDS) manage cryptographic keys. The documents do not, therefore, allow a reader to determine what might happen if an attacker discovered the key used by one Edge unit, e.g., whether discovering the key in one Edge unit would leave other machines vulnerable. A report commissioned by Alameda County found that these keys are in fact constant, which could allow an attacker who discovers the keys on one Edge to attack other Edge units.[100]

- The same report for Alameda County states that it is possible to copy a results file and the corresponding cryptographic hash value from one results cartridge to another. The result of this attack would be that the results file of the destination cartridge would be overwritten and not tallied.[101]

- The documentation provides little discussion of the environment in which the AVC Edge might be operated, primarily in precincts on election day and in early voting locations.

- The Operators Manuals for the AVC Edge, the HAAT, and the Card Activator contain essentially no information about security.

The Sequoia system documentation also presents some security analysis of the devices that support the Edge—the Card Activator, the HAAT, and the VeriVote printer—though this documentation is less extensive than it is for the Edge. In particular, of these three devices, only the HAAT has its own Security Specification.[102] Neither the VeriVote nor the Card Activator appears to have a security overview or similar document.[103]

HAAT The HAAT test report presents more specific information about how testing was performed than other ITA reports for the Sequoia system, but details about security testing are still scarce. For reasons not explained in the documents, the HAAT was submitted for qualification testing separately from the AVC Edge. Indeed, the HAAT was tested by a separate ITA.[104] The HAAT, however, was part of the voting system that was integration tested by the software ITA.[105] The report does not state whether the integration test involved the HAAT 50 or the

[99] *Id.* at 7.

[100] *See* Craig Humphreys & Craig Merchant, Sequoia Voting Systems Vulnerability Assessment and Practical Countermeasure Development for Alameda County iii, Oct. 4, 2006, http://accurate-voting.org/wp-content/uploads/2006/10/alameda_sequoia_vuln.pdf.

[101] *Id.*

[102] We were provided with version 1.00 of the HAAT Security Specification, dated August 2006. Systest, which reviewed the HAAT and issued its report on February 3, 2006, does not list a HAAT Security Specification as a reference. *See* Systest Labs, Independent Hardware Test Report for Sequoia Voting Systems Hybrid Activator Accumulator & Transmitter (HAAT) Unit, version 1.0.69L (rev. 04) § 3.5.

[103] This statement is based on our review of all of the Sequoia documentation that we received and an examination of the references in the AVC Edge ITA report ("5.0.14 Report"). *See* 5.0.14 § 2.0 (listing the VeriVote Printer Operators Manual, Maintenance Manual, and Test and Verification Specification as references for the VeriVote; and the Card Activator Operators and Maintenance Manual, Software Specification, and Poll Workers Manual).

[104] Systest tested the HAAT, while Wyle tested the AVC Edge, VeriVote, and Card Activator, all of which were submitted together.

[105] *See* Software Qualification Test Report: Sequoia WinEDS 3.1.012 (rev. 1.0), Feb. 15, 2006 (listing HAAT, firmware version 1.0.69L, as a system component).

HAAT 100. As stated in section 2.3, one difference between the HAAT 50 and HAAT 100 is that the HAAT 50 can load configuration information only via a USB port, while the HAAT 100 can use either a USB port or a PCMCIA slot.[106] The WinEDS ITA report's description states only that the "[e]lection was loaded in the Edge and HAAT card activators from the prepared cartridges."[107] The reference to "cartridges" is ambiguous because the Sequoia documentation refers to both USB and PCMCIA-based storage media as "cartridges."[108] The WinEDS ITA report also notes that the functional testing involved consolidating results on the HAAT—a function that only the HAAT 100 can perform—but this does not rule out the possibility that the HAAT 50 was also used the integration testing.[109] As the Sequoia Red Team and Source Code Review Teams detail in their reports, the HAAT's USB port plays a role in a potential attack against the Sequoia system.[110]

Based on the test descriptions in the HAAT ITA Report, the HAAT's USB ports received little, if any, attention during security testing. The HAAT ITA Report describes in some detail the tests that the ITA performed to evaluate HAAT security; this description does not mention the USB ports.[111] Similarly, the VSUP and OVSTA Memo overlook potential threats arising from the use of USB keys in conjunction with the HAAT and provide no specific procedures to manage them.[112] The HAAT Security Specification does addresses this type of threat only by asserting that it is "not possible to introduce executable code into the HAAT via a USB . . . Preparation Cartridge, either at election setup or at any other time."[113] The HAAT ITA Report offers no independent evaluation of this claim. Moreover, this claim is inapplicable to the kind of threat identified by the Red Team.

VeriVote Printer VeriVote procedures documents contain little explanation of how the VeriVote relates to security. For example, the VeriVote Pollworker Guides for Assembly and Disassembly instruct pollworkers as to how to handle the security seals that are designed to break if the printer cover is opened or the printer is detached from the Edge unit.[114] The VeriV-

[106] *See* HAAT (Hybrid Activator Accumulator & Transmitter) Operations & Maintenance Manual § 4.3 (rev. 1.09), Jan. 2006 ("*NOTE: HAAT50 Units can be prepared using USB Preparation Cartridges ONLY.*") (emphasis and capitalization in the original).

[107] *See* WinEDS ITA Report at 86-89 (describing test cases used for functional testing of the integrated system).

[108] *See supra* note 106.

[109] *See* WinEDS ITA Report at 93 (describing "HAAT Consolidation"); HAAT Operators & Maintenance Manual, *supra* note 106, § 2.5.3 (noting that consolidation is only available for the HAAT 100).

[110] *See* Sequoia Red Team Report and Sequoia Source Code Review Team Report. The USB port is the only way to prepare the HAAT 50 with ballot definitions. Sequoia Voting Systems, HAAT System Overview § 2.1.9 (rev. 1.08), Jan. 2006.

[111] *See* HAAT ITA Report App. E. The security test described in the most detail was designed to determine whether the HAAT 100's wireless modem encrypted data during transmission and handles SSL certificates in the expected manner. *Id.* Since the HAAT 100 is not part of the Sequoia system certified for use in California, this test is inapplicable to this review.

[112] As we discuss in the Usability section, the Sequoia system documentation does not explain how to transfer ballot definitions to the HAAT 50 via the USB key; we relied on an explanation from a Sequoia technician to learn how to do this.

[113] HAAT Security Specification § 1.3.1.

[114] *See* AVC Edge with VeriVote Printer Pollworker's Guide Booklet 2 (Setting Up Voting Equipment & Operating Polls) 16, 21 (rev. 2.01), Dec. 29, 2005; AVC Edge with VeriVote Printer Pollworker's Guide Booklet 4 (Closing Polls & Disassembling Voting Equipment) 8 (rev. 2.01), Dec. 29, 2005.

ote pollworker guides do not relate security seals to the security of the printers or their role in voting system security overall. Perhaps this level of detail would not be appropriate for a pollworkers guide. But these documents simply tell pollworkers when to break the VeriVote's security seals; thus, they assume that a pollworker will not unexpectedly find a broken seal. Though procedures for handling this situation will likely vary from jurisdiction to jurisdiction, these pollworker guides could create some awareness of security by instructing pollworkers to consult officials in their precinct if they find a broken seal.[115] Other potential contingencies on election day – such as the need to replace a VeriVote paper roll – are handled in the Maintenance and Operators Manual, where they are severed from the security context provided by tamper-evident seals. The VSUP and the OVSTA Memo provide detailed procedures for logging security seal serial numbers if a paper roll must be changed,[116] but none of the documentation addresses the possibility of finding a broken seal.

Card Activator The Sequoia Card Activator documents—the Operators and Maintenance Manual,[117] the Pollworkers Manual, and the Software Specification—contain no reference to voting system security. We also were not able to determine from the AVC Edge ITA report what kinds of security testing and review were performed as part of the system's qualification testing. This overall lack of attention to Card Activator security is consistent with one of the findings of the Sequoia Red Team Report, which notes that the screws holding the Card Activator's case together are easily removed and are unprotected by security seals.[118]

Physical Security and Security Procedures The primary source for procedural and administrative safeguards for the AVC Edge is the Voting System Use Procedures (VSUP) for California. Security in the VSUP is a separate chapter, as required by the Voting System Use Procedures for California Template; this separates the security procedures from the specific election phases to which they apply. The security procedures for the Edge fall into several categories: attaching serial numbers to memory cartridges; pre-election LAT; chain-of-custody and physical security of the Edge, memory cartridges, and VeriVote printers; and user-level security.

Most of these procedures are organized under headings that express a general class of security threat, e.g., "protection against malicious software."[119] This organization provides more coherence than the AVC Edge Security Overview, for example, which claims security properties for the Edge in the absence of any discussion of specific types of security threats. Still, the document is not self-contained and is somewhat byzantine. The VSUP refer the reader to a number of other documents for information about how to complete certain tasks.

[115] This method for handling the possibility of county-specific procedures is found elsewhere in the VeriVote Pollworker guides. The Assembly Guide, for example, incorporates some variations for county-specific uses of padlocks to secure the printer to the Edge. See VeriVote Printer Pollworker's Guide Booklet 2 – Setting Up Voting Equipment & Operating Polls 20 (rev. 2.01), Dec. 29, 2005.

[116] VSUP App. K.2.3; OVSTA Memo ¶ 7.

[117] The VSUP refers the reader to the Operators & Maintenance Manual for Card Activator procedures. *See* VSUP § 4.8.2.

[118] *See* Sequoia Red Team Report.

[119] VSUP § 10.1.8.

Finally, the audience for the VSUP is unclear but appears to be election officials. It would be worth considering whether requiring security procedures to be integrated into the chapters for specific election phases would make this document more useful to that audience. The timing of the VSUP's release might also present an issue for election officials who must follow its guidance. The VSUP, though required as a condition of the Sequoia system's March 2006 certification, do not appear to have been released until October 2006.

4.2.8 Auditing

Auditing is a key element of voting system security. The scope of a full audit would go well beyond the mandatory one-percent post-election recount required by California Elections Code § 15360, toward a reconstruction of key events during an election.[120] In order for such an audit to be possible, the relevant data must be recorded, and those records must be kept secure. Relevant data include individual ballots; post-election precinct vote reports; chain-of-custody records for voting machines, removable media, and security seals; VVPAT rolls; and audit and event logs from voting machines and the EMS server.[121] The security of records relevant to an audit, moreover, involves not only keeping them secure once they reach a storage facility, but also ensuring that the people who handle the records are aware of the importance of adhering to protocols that establish and preserve the records' integrity. The auditing capacities of the various pieces of the Sequoia system were described in chapter 2.

Our key findings with regard to auditing are:

1. The documentation for the AVC Edge and WinEDS is insufficient; we were unable to determine from the documentation how to perform important audit-related functions.

2. The documentation for the Optech Insight provides insufficient guidance to pollworkers as to how to handle the printed audit tape.

3. The VSUP procedures regarding the mandatory post-election one- percent audit are incomplete.

AVC Edge We encountered the difficulties with the AVC Edge event log during our second session with the Sequoia equipment in Sacramento. Prior to arriving in Sacramento, we had found that the documents described a *use* for an Audit Trail Transfer Cartridge but did not describe how to prepare one. Given the importance of this cartridge—it is the only way to transfer the Audit Trail contents (including the Edge's event log) if the Results Cartridge is lost—we attempted to improvise a procedure. Basically, this procedure was the same as creating a Results Cartridge, except that we selected the "Audit Transfer" cartridge type, in WinEDS, rather than the Results Cartridge type. We provide additional details in section 4.1.5. WinEDS did not generate any error messages during this process.

After following the AVC Edge Operators Manuals instructions for using the Audit Trail Transfer cartridge, however, we were unable to complete the task of copying the Audit Trail

[120] *See, e.g.*, Collaborative Public Audit of the November 2006 General Election Report of the Public Monitor of Cuyahoga County, Ohio, Apr. 18, 2007.

[121] *See id.*

contents to the cartridge. Although we succeeded in following all steps up to the point that the Audit Trail should have been copied (according to the Operators Manual), the Edge unit did not recognize the card and prompted use to remove it. Neither the error messages on the Edge nor the documentation explained what the problem was.

Insufficient Optech Insight audit tape procedures As noted above, maintaining the integrity of printed and electronic event log records from voting equipment is essential to the effectiveness of a post-election audit. We found, however, that the Optech Insight Plus Pollworkers Guide (PWG) does not provide sufficiently clear guidance about how to maintain this integrity in the context of a polling place on election day.

In particular, pages 32-36 of the PWG describe error messages that a pollworker might encounter as ballots are scanned—in the presence of the voter—by the Insight Plus on Election Day. This section of the PWG does not contain any warnings against tearing the error tape to allow the voter to understand the source of the error. Based on our use of the Insight Plus during the first walk-through, we believe that this is a reasonable impulse. A pollworker might, for example, conclude that tearing the tape and handing it to the voter would protect the secrecy of the ballot. Despite warning against this in the prior chapter, which describes how to open the polls, the PWG omits this warning in the election day chapter. Procedures and instructions given in the polling place provide this warning, but the PWG does not.

Inaccurate information about 1% manual tally Finally, the VSUP's procedures for conducting the mandatory one-percent recount omit crucial information, and, for this reason, we find that they are insufficient.[122] Specifically, the VSUP sets a deadline for the random selection of precincts that does not comport with California law; the VSUP states that election officials should randomly selection precincts to be "within fifteen days after every election." California's automatic recount law does not impose a deadline to select these precincts;[123] instead, the law requires the selection and auditing of precincts "[d]uring the official canvass of every election in which a voting system is used."[124] Sound recounting procedures require election officials to wait until all ballots have been tallied to select the precincts to be recounted. Otherwise, it becomes possible for an attacker to corrupt votes in precincts that are known not be on the recount list. This, in turn, would diminish the effectiveness of the audit as a deterrent against such attacks, as well as its effectiveness in detecting them if they are actually carried out.

[122] The manual recount procedures are given in § 9.1 of the VSUP.

[123] The statement in the VSUP appears to reflect an outdated version of the automatic recount law. From 1994 to 1998, Cal. Elec. Code § 15645 specified: "Within 15 days after every election in which a voting system is used the official conducting the election shall conduct a public manual recount of the ballots tabulated by those devices cast in 1 percent of the precincts chosen at random by the elections official." This requirement was repealed, and § 15360 was enacted, in 1998. *See* 1997 Cal. SB 627 and Stats. 1997 ch. 1073.

[124] Cal. Elec. Code § 15360.

4.3 Ballot Secrecy

The California Constitution and the California Elections Code guarantee the secrecy of the ballot.[125] Similarly, the VSS provide require that "all systems shall . . . Protect the secrecy of the vote such that the system cannot reveal any information about how a particular voter voted, except as otherwise required by individual State law."[126] The VSS provide more functional requirements for ballot secrecy on a DRE such as the AVC Edge: the machine must clear all ballot selections from the display and any memory or other form of storage, other than storage that is specifically allocated for recording ballots.[127] Canceled ballots must be handled similarly, except that the DRE must erase all data immediately.[128] In addition to these specific requirements, the VSS state that DRE systems shall "[p]rotect the secrecy of the vote throughout the voting process."[129]

The documentation for the AVC Edge reflects a broad array of possible threats to ballot secrecy. The first set of threats concerns ballot secrecy at the polling place. For each of the VSS' secrecy-related requirements, the AVC Edge ITA report notes that these parts of the voting system were "accepted." This report notes the presence of privacy panels surrounding the Edge's touchscreen and on the VeriVote printer.[130] Beyond this, however, the ITA report does not explain how the ITA concluded that the data deletion requirements were tested or how the requirements relating to ballot secrecy throughout the election process.[131]

Sequoia's Test and Verification Specification does little to clarify how the ITA might have performed its tests. This specification simply directs the test lab to "[v]erify that the AVC Edge allows voters to vote in secret, and preserves the secrecy of the ballot." [132]

Other polling place threats to ballot secrecy arise specifically from the need, under some circumstances, of pollworkers to interact with DREs and even to take actions with an individual ballot. The AVC Edge Operators Manual specifies three situations in which a pollworker needs to intervene in the use of a DRE. In none of these situations does the Operators Manual mention that the pollworker should be aware of ballot secrecy and attempt to minimize the potential for seeing a voter's selections:

- An invalid voter card. The Operators Manual states that a pollworker will eject the card by pressing the Activate button.[133]

- A voter leaves without making a selection. The Operators Manual states that a pollworker may either allow voting to continue, cast the ballot, or cancel that voter's activation.[134]

[125] California Constitution, art. 2, § 7 ("Voting shall be secret."); Cal. Elec. Code § 19205(b) ("The [voting] system shall preserve the secrecy of the ballot.").

[126] VSS Vol. I, § 2.4.3.1

[127] VSS Vol. I, § 4.5.a.

[128] VSS Vol. I, § 4.5.b.

[129] VSS Vol. I, § 2.4.3.3.q). *See also* § 3.2.4.1 ("Provide privacy for the voter, and be designed in such a way as to prevent observation of the ballot by any person other than the voter") and § 3.2.2.2 (space requirements to preserve privacy) and requirement for audio privacy.

[130] 5.0.14 Report §§ 4.1.1-4.1.2.

[131] 5.0.14 Report at A-26; *id.* at A-11.

[132] AVC Edge Test & Verification Specification § 3.16.

[133] AVC Edge Operators Manual § 4.3.5.

[134] AVC Edge § 4.3.5.

The VSUP and AVC Edge Election Day Support Manual appear to combine procedures for a blank ballot this has been left by a voter and the situation in which a voter requests assistance in casting a blank ballot.[135]

- A voter "flees" the polling place after making at least one selection. The Operators Manual states that a pollworker may choose to cast the ballot or return to voting.[136] The Use Procedures, however, instruct the pollworker to cast the ballot.[137] If California law requires the fleeing voter's to be cast, the VSUP should make clear that its guidance is what the pollworker must follow.

The Election Day Support Manual presents additional scenarios in which pollworkers may need to interact with a DRE: when a voter believes that his or her ballot was not cast, and when the Edge gives a vote save error after the voter casts the ballot.[138] Neither of the procedures for these situations mentions ballot secrecy.

The second set of ballot secrecy threats arise from reporting and auditing procedures. The ballot secrecy problems with VVPAT rolls, which record ballot information serially, have been widely noted; but the documents do not discuss this issue. It would be helpful to see an explanation of how chain of custody procedures, for example, might mitigate threats to ballot secrecy. A second example is the requirement that precincts post vote reports from each voting machine at the close of an election. This is a potential threat to secrecy if few voters used a machine. To address this problem, the OVSTA Memo directs pollworkers not to post Edge results for machines used by only one or two voters.[139] Third, there is little mention of VVPAT bar codes in the documentation. The VeriVote can print a bar code,[140] but none of the documents discuss whether or how to disable this feature. The system documentation should provide this information.[141] Finally, the documentation notes that the Edge stores ballot records in blocks of memory that are chosen at random.[142]

This section has pointed out contexts in which ballot secrecy is an issue but receives no explicit mention; overall, the documentation contains little or no discussion of the issue. For these reasons we find the documentation to be insufficient with respect to ballot secrecy.

4.4 Reliability

Reliability is defined in the VSS to mean "the mean time before failure . . . for the system submitted for testing."[143] We expand this definition slightly, to include the ability of a

[135] *See* VSUP App. H.3.4; AVC Edge Election Day Support Manual § 2.6.1.

[136] AVC Edge Operators Manual § 4.3.5.

[137] VSUP App. H.3.5.

[138] AVC Edge Election Day Support Manual §§ 2.2-2.3.

[139] OVSTA Memo ¶8.

[140] VeriVote Printer Maintenance Manual 3-2, rev. 1.05, May 2005.

[141] We were also unable to find in the documentation a clear statement of whether printing bar codes on VVPAT records is permissible under California law. This is an area in which additional guidance from the Secretary of State would be welcome.

[142] *See* AVC Edge Functional Specification § 6.9; AVC Edge System Overview § 2.13.

[143] VSS Vol. I, § 3.4.3. The mean time before failure, in turn is defined as "the value of the ratio of operating time to the number of failures which have occurred in the specified time interval." *Id.*

system or component to warn a user about actions that will crash the system or result in data loss. Of particular concern in the voting context are actions that could take a machine out of service on election day or which could cause the loss of election data. In this section we discuss whether the Sequoia documentation provides adequate information to allow a reader to determine whether the system is reliable, and under what conditions.

The documents provide several types of data to support the basic reliability of hardware in the Sequoia system. The ITA reports, for instance, conclude that the Sequoia optical scan and DRE equipment withstand such environmental stresses as electrical surges, temperature extremes, high humidity, and magnetic fields. Moreover, the ITA reports refer to specific standards that describe how these tests were performed and usually include original data from the tests.

In addition, the volume tests for the Edge and the Optech Insight provide most of the information necessary to determine how testing was conducted, which errors were encountered, and how they were explained.[144] The Sequoia Staff Report states that 100 Edge I, 100 Edge II, and 50 Optech scanners were used in the volume tests, but the Report does not state how many votes were cast on each system and over what period of time. Without this information, it is difficult to get a sense of the rate of the two errors reported in the Edge II[145] testing that were not related to either human error or vote activation card failure.[146] The Sequoia Staff Report states how these errors manifested themselves and how the testers resolved them. Similarly, the Report states how many paper ballots became jammed in the Optech Insight and Insight Plus units during volume testing; but it does not state the percentage of ballots that jammed.

In other areas of reliability, however, the documentation was not complete. Prior to resetting the AVC Edge, the system warns simply warns that it is ready to reset and asks, “Are you sure?” The Operators Manual explains the consequence of a system reset: It clears the Audit Trail memory, including ballot data.[147] Furthermore, the Operators Manual implores the reader to “be sure,” as the reset is irreversible.[148] The VSUP contains the same instruction.[149] These documents do not explain the circumstances under which a system reset is appropriate, or whether a state or jurisdiction might have laws or regulations in place to control an action that erases ballot data. Though it may be beyond the scope of the Sequoia documentation to specify these considerations, it could provide a warning that points in the right direction. The Edge poses the same question before it carrying out an Audit Trail transfer. The question, “Are you sure?” is more perplexing in this context. The VSUP states that this function transfers a copy of the Audit Trail to a memory cartridge, so this operation would appear not to destroy data.

WinEDS raises a different set of reliability issues because of its role as the central nervous system of the Sequoia voting system. There are several issues to consider when looking at the possibilities for user error and eliminating potential issues that could cause problems with the database and vote integrity. The complexity of the WinEDS program requires up to date and

[144] *See* Sequoia Staff Report at 9-13. Note that we do not address the adequacy of the volume tests, but rather the question of whether the documents provide the reader with an understanding of how the tests were conducted.

[145] The Edge I volume test generated only human errors and vote activation card errors. One error on the Edge II involved the unit’s failure to record a vote successfully. The other was a paper jam on the VeriVote printer.

[146] Sequoia Staff Report at 10.

[147] AVC Operators Manual § 4.3.10.

[148] *Id.*

[149] VSUP App. E.2.4.

detailed manuals to assist users in their work.

The user interface presents another possibility for human error. One remedy is to simplify the process for creating and tallying an election to allow for easier auditing and less confusion when using the interface. WinEDS addresses this concern by providing wizards, which allow users to walk through steps in order to configure certain processes. The data wizard is particularly problematic when run as administrator, as certain settings that are misunderstood or selected during the wizard have the potential to damage the system.

Process and access issues are another concern for human error. The documentation must describe what parts of the process are to be performed by what roles. Additionally, issues around the integrity of the computer that WinEDS is installed on, as well as the data it is using must be addressed by process as well.

4.5 Accuracy

4.5.1 Optech Insight and 400-C

Voter Feedback

Due to the paper based nature of optical scan technology a failure of, or an attack on, the software or hardware of the system can be recovered from by hand counting the actual ballots. However, the likelihood of detecting different kinds of machine failures is greatly reduced in the context of the 400-C because as a central count machine, in which ballots are fed by an election official, it does not provide for voter feedback. The lack of voter feedback in the 400-C and other central count systems reduces the opportunities for errors in ballot marking to be addressed by the voter prior to casting or when problems with marking devices, calibration or other system wide issues can be identified and eliminated. Precinct-based systems such as the Insight and Insight Plus, when configured to return over- and undervoted ballots, blank ballots, and other unprocessable ballots, provide an opportunity to maximize the opportunity for voters to decisively convey their intent in a manner that will be accurately detected and recorded by the machine. Through voter feedback due to ballot rejection they also provide an opportunity to proactively identify systemic problems with the voting system.

Ballot Reading Technology

A primary source of accuracy problems, defined as a failure to capture voter intent, is limits on the optical scan system's ability to identify marks that indicate a voter's intent to cast a vote. Optical scan systems can only count marks that they can detect. Within the range of what they can detect then can be configured with differing sensitivity that controls the number of false positives (marks that are recorded as votes but that do not meet the legal definition of an acceptable mark) and false negatives (marks that are not recorded but meet the legal definition of an acceptable mark).[150]

The 400-C uses infrared sensing technology. Because this is a range of light that is not visible to the human eye, marks that are evident to voters and pollworkers may on occasion

[150] For a rich description of the issues in optical scan systems see Douglas W. Jones, Counting Mark-Sense Ballots: Relating Technology, the Law and Common Sense, http://www.cs.uiowa.edu/∼jones/.

not be detected by the sensors. On the other hand, ballot marks imperceptible to the voter or pollworker may be detected and tabulated by the sensors. Thus, a primary concern is making sure that the ballot marks are perceptible to both the human eye and the infrared photosensors in the 400-C. This is particularly important because the voter is not provided with feedback and an opportunity to correct for under or over votes which may be caused by the use of an inadequate ballot marking device, or inadequate marking of the ballot with an otherwise acceptable marking device.

The Insight and Insight Plus (Insight) use visible light-emitting diodes and photosensors. This eliminates the possibility that ballot marks made by voters will be technically imperceptible to the machine due to the fact that the optical scan sensors and the human eye are sensitive to different wavelengths of light. In addition, the precinct-based context of the Insight use protects against over and under votes caused by inadequate, duplicate, or stray markings. Blank, under and over voted ballots are all returned to the voter with an error message indicating the reason for the failure to read. Voters are presented with a range of options where ballots are returned.

Both the 400-C and Insight use the broken arrow ballot format. The broken arrow style of ballot maximizes the ability of the sensors within the scanners to reliably detect marks indicating voter intent where they do not fill the entire target area for the contest.

The use of the broken arrow ballot style in conjunction with voter feedback in the case of the Insight, are checks on the accuracy with which the optical scan system captures the voter's intent. With respect to the 400 C the election worker is provided feedback on cast votes.

Testing at the federal and state level is not currently designed to determine the ballot marking implements that optimize the Insight and 400-C's ability to read ballots. The test reports for the Sequoia optical scanners did not state whether the ITAs examined this issued and, if so, the extent and form of their testing.

The calibration of the scanners is critically important. If the scanners are set to read very faint marks, they may interpret stray marks as indicating vote choices, complicating ballot processing or, potentially, causing an inaccurate recording of voters' intentions. Overall, the Sequoia documentation does not sufficiently describe and explain all relevant aspects of optical scan calibration and use. The documentation for the 400-C does provide detailed instructions for calibrating the read head to prevent it from reading the faintest marks on a test ballot.[151] Beyond this, however, the documentation left many unanswered questions about the technology. In particular, the documentation does not provide clear guidance about which kinds of marking implements will produce ballots that are most likely to be read accurately. The Maintenance Manual for the 400-C states that "the optimum marker to use is a fine or medium felt tip marker with black or blue ink"[152] but goes on to say that "voter instruction blocks on official ballots *should* instruct the voters to mark their ballots with #2 soft lead pencils."[153] Still later, the Maintenance Manual states that the 400-C is "blind to most red pens or pencils . . . and [is] known not to read certain 'BIC Biro' ballpoint pens, as well as certain 'Highlighter' felt tip pens."[154] It then reiterates that blue or black ink is an "optimum marker," but once again

[151] Sequoia 400-C Ballot Counter System Maintenance Manual § 5.3, rev. 1.01, July 2003.

[152] Sequoia Voting Systems Optech 400-C System Overview § 3.8, rev. 1.01, Jan. 2005

[153] *Id.*

[154] *Id.* § 5.4.2.

recommends instructing voters to use #2 soft lead pencils.[155]

Thus, the documentation is internally contradictory on a key issue of accuracy. It should be edited to provide clear, consistent guidance to help voters use the most accurate voting implements. Placing this guidance in a document other than a maintenance manual—which might not be routinely read by election officials—should also be considered.

Similarly, the documentation does not provide information about the criteria used by the ballot tabulator to distinguish between acceptable and unacceptable marks. The documentation for the 400-C and Insight provides information that describes the columnar areas of the ballot in which the sensors will detect marks,[156] however it does not provide sufficient information about the upper and lower bounds within the columnar area that will be detected for each target.[157] Finally, while the directions to voter provide some guidance on the sort of marks voters should place on the ballot, the system documentation provides insufficient information distinguishing between reliably detected and reliably ignored marks.[158] "Ideally, the documentation for the scanner should include samples of each class of mark. These serve to illustrate, by example, the criteria the system uses, and they also serve to illustrate how close to marginal the prescribed mark is and how reliably the system is in ignoring marks such as erasures and hesitation marks."[159]

Testing documentation provides inadequate information about the extent of testing of machine calibration and sensitivity to marks. The California state reports indicate some testing of various marks, while the federal testing provides no indication of such tests and a check-box format for assessing compliance with existing VSS guidelines and no indication of the tests actually run.[160]

[155] *Id.*

[156] Optech 400-C System Overview §3.3.2 explains that the infrared LEDs identify the heads and tails of arrows that are used to orient the read area of the visible red LEDs; Sequoia voting Systems Optech Insight Plus Hardware Specification, Document Version 1.01, September 2005, Part Number 190-32823-00, §2.3.5, p. 2-6 similarly describes the use of two sensing channels to identify the heads and tails of the arrows and the third to identify marks.

[157] If you conceive of the target area as a box, the documentation provides information about the outer bounds of two sides of the box while leaving the outer bounds of the top and bottom undefined (although perhaps decipherable based on the read frequency of the heads (the sampling rate) and the processing speed of the machine) and subsequently the bounds between marks unknown, i.e,. will a mark mid-way between two arrows be considered a viable mark for one, the other, or no contest.

[158] *Id.*

[159] *Id.* Douglas W. Jones, Counting Mark-Sense Ballots: Relating Technology, the Law and Common Sense, http://www.cs.uiowa.edu/∼jones/.

[160] Sequoia Voting Systems Inc. Staff Review and Analysis, February 22, 2006, p. 31 documents that on January 26, 2006 "specially mark ballots (unusual marks, assorted pens)" were tested on the 400-C, Insight and Insight Plus, however there is no information about the actual marks and pens tested, nor the test outcomes. In contrast, it is completely unclear what tests were done to assess calibration, interaction with marking devices, and deviations in read ranges in the federal testing. The documentation for the Insight and 400-C include a check box list which indicates that § 3.2.5.2 of the VSS standards for Ballot Reading Accuracy were met, however the requirements state that the system detects marks that conform to the vendors specifications within an acceptable error rate, ignore extraneous perforations, smudges and folds, and has a 2% or less rejection rate for conforming ballots. This does not provide information about what marks are considered to "conform to the vendors specifications" nor does it indicate what tests were used to make these assessments. For example, see, Preliminary Test Report, Sequoia Voting Systems Hardware Qualification Testing of the Sequoia Optech 400-C Ballot Counter (Firmware Version 1.12.4) Wyle Laboratories Inc. 1/12/06, Test Report No. 52125-04 p. A-23.

In the absence of this information election officials are under-equipped to make decisions about optimal ballot marking devices, advise voters about adequate ballot marks, and make decisions about how to calibrate their own machines.

Given that optical scan machines cannot duplicate the nuanced capacity of humans to discern indications of "voter intent," the goal should be to reduce stray and inadequate marks through voter education and where over-voted, under-voted and blank ballots are detected return them to the voter to provide opportunities for correction. Without adequate information about the underlying technology and testing it is difficult for election officials to make determinations about voter education and ballot marking devices. The current design and configuration of the 400-C and Insight in California separate out over-voted, under-voted, and blank ballots so that they may be separately subjected to a manual examination to discern voter intent. This is an important check due to the inadequacy of documentation with respect to the outer-limits of top and bottom edges of the target areas for ballot marks, the lack of full information about the spectral response of the system, and the inherent gap between machine processing and human processing with respect to deriving voter intent.

4.5.2 AVC Edge

The primary check that the AVC Edge records ballots that reflect the voter's intent is the VVPAT. Several documents explain that the AVC Edge can be configured to require a paper record to print before the voter is allowed to cast his or her ballot, and the Edge that the Document Review Team used during its walk-through was configured this way. The documents do not state, however, whether the AVC Edge or the VeriVote printer will give any warnings or prevent a voter from casting a ballot if the paper feed is jammed.[161]

[161] *See, e.g.*, AVC Edge Operators Manual at 71 (listing event log entries relating to the VeriVote printer but omitting mention of a paper jam).

Chapter 5

Conclusion

We have found that the documentation for the Sequoia voting system is incomplete. The documentation, taken as a whole, fails to provide evidence that all applicable requirements of the VSS were tested during the system's qualification tests. The incompleteness of the documentation in this regard is particularly acute for WinEDS; the ITA report for that component does not state with specificity which requirements were tested. The other ITA reports provide this specificity but do not detail the tests that they used to determine compliance with the standards. Finally, documentation for the course of testing the AVC Edge is highly incomplete.

- **Suggestion:** Obtaining reports for all submissions of a voting system to a testing lab, test plans, and documents that vendors submit at the testing lab's request (such as penetration analyses) would shed considerable light on how the labs test voting systems under the applicable standards.

We also found that the Sequoia documentation is insufficient in a number of important ways. We were able to use the documentation to perform major steps in an election, but we encountered a few significant usability problems in doing so. More generally, we found the extensive cross-referencing of documents to be an impediment to using them efficiently. This was particularly true of the Voting System Use Procedures for California.

- **Suggestion:** Evaluate whether the template for the Voting System Use Procedures yields documents that are sufficient to meet the needs of the Secretary of State as well as election officials.

Finally, we found the that documentation did not provide information about security, ballot secrecy, reliability, and accuracy that was sufficient to allow an election official or pollworker to understand the range of threats to those aspects of voting system performance and how to mitigate against them.