DOCUMENTATION REVIEW
OF THE
HART INTERCIVIC SYSTEM 6.2.1 VOTING SYSTEM

Joseph Lorenzo Hall
University of California, Berkeley*

Laura Quilter
University of California, Berkeley*

July 20, 2007

* Affiliations are provided for identification purposes only.

Table of Contents

1 Executive Summary

This report evaluates the documentation in the possession of the California Secretary of State for the Hart InterCivic ("Hart") System 6.2.1. The report was prepared on behalf of the California Secretary of State's "Top to Bottom" Review ("TTBR") of voting systems used in California. The entire project involved assigning four teams to each system. One team studied the source code of the system ("source code team"), a second team conducted "red team" exercises against the actual systems as they might be deployed in the field ("red team"), a third team assessed the degree of accessibility of the system ("accessibility team"), and a fourth team studied the documentation of and for the system. This report describes the findings of the Hart Documentation Team.

The Hart InterCivic 6.2.1 system is comprised of a suite of precinct-level proprietary voting system components running proprietary software (Judge's Booth Controller ("JBC"), eSlate, eSlate/DAU and eScan), and a back-office Windows-based election management system (the "Hart Election Management System" ("HEMS"), including the eCM Manager, BOSS, Ballot Now, SERVO, Rally, and Tally). The back-end software is used to define the election database, manage the election and equipment, and tabulate results. The precinct-level devices present ballots to the voters and collect and store ballot information while polls are open. Election data is transported from the proprietary hardware to the HEMS on removable PCMCIA memory cards ("Mobile Ballot Boxes" ("MBBs")), or optionally transmitted via modem or local network. The PCMCIA cards and USB security keys, called "eSlate Cryptographic Modules" ("eCMs"), are critical third-party products used to store election data and security data, respectively.

1.1 Document Review Goals and Findings

We designed our review, given constraints, to provide answers to the following questions:

1. Are the ITA reports sufficient to demonstrate or provide credible evidence that all VSS requirements were tested and to provide enough information to independently judge whether the ITA tests were appropriate for the task?

   Disposition: The national certification reports largely fail to communicate information one would need to assess the systems with respect to the Voting System Standards. In many cases, especially with non-environmental tests, it is difficult or impossible to determine what testing methodologies were employed, the detailed results of this testing, and what actions and resources an independent evaluator would need to replicate their results. In some cases, relevant items in the Federal Election Commission's (FEC) Voting System Standards 2002[1] (VSS) were not tested at all or the division of labor between two testing laboratories contributed to serious deficiencies. The state consultant reports, while also not providing enough information to replicate their tests, did carefully document serious issues that seem to have slipped through the cracks of the national certification process.

[1] Voting System Standards 2002, Federal Election Commission, April 30, 2002, *available at:* http://www.eac.gov/election_resources/vss.html (DOC) *or* http://josephhall.org/fec_vss_2002_pdf/.

2. Is the system documentation usable for election administrators and poll workers?

   Disposition: Broadly speaking, the Hart system documentation for users (election officials, support personnel, pollworkers) is adequate to establish and run an ordinary election in which few or no problems occur. The documentation is relatively well organized and versioned with explanations as to the differences between versions. However, the documentation fails to anticipate or document some common problems and exceptional events.

   There are a number of areas in which the documentation should be improved. While the Hart Use Procedures provide a good high-level description of running a Hart election in California, the operations manuals for the Hart system contain mostly atomic, step-wise descriptions of how to perform specific actions; there is little in the way of material that might help jurisdictions connect these detailed steps to the bigger picture, and incorporate California-specific requirements.

   Hart's documentation is highly referential, referring to other documents frequently that the user may or may not possess. This can pose problems given time and resource constraints if problems arise that could be easily answered with missing documentation. This issue is especially acute for the *Hart Use Procedures* that govern the use of the Hart system in California. The Use Procedures documents are public documents, and members of the public are poorly served by references to proprietary or otherwise non-public documents. We recommend that Use Procedures documents be designed to provide a more self-contained set of procedures.

   Hart's documentation largely describes *how* to do things. Rarely does it describe why one might want to do something, what the implications could be, or technical details of exactly what is happening, for users that might be interested in issues of security, accessibility, reliability and auditability. We recommend that vendors provide a channel of communication so that their users, at all levels of technical sophistication, can describe what would be useful to them in the documentation.

3. Is the system documentation complete enough for counties to be reasonably self-sufficient in running an election? Would counties need extensive technical support from the vendor?

   Disposition: Assuming that a jurisdiction using the Hart system had knowledgeable and competent technical staff, we believe they could run an election with little or no assistance from Hart. We base this finding on walkthroughs we conducted in Sacramento with the equipment. We ran two mock elections over a period of five hours and were able to exercise most of the Hart system's major functionality with little trouble. That said, we recommend that jurisdictions "break in" their internal processes by running mock elections in an environment as close to a real election as possible to increase staff experience with the system and to become familiar with any quirks of the system as currently certified.

4. Were the documents complete enough for state officials to have the information they'd need to make certification decisions?

Disposition: We do not believe that the documentation we were provided for our review would be sufficient for state officials to make informed certification decisions. The inadequacy of information provided at the national certification level—the poorly documented testing reports and the complete lack of detailed test plans—combined with the highly referential nature of Hart's documentation put state-level certification at an information disadvantage. The TTBR teams had access to all the documents in the Secretary of State's possession and still did not have all the documents it needed (see section 4.1.1). Part of the solution here is an improved national certification process, which is currently evolving now that the responsibility for that process has changed hands. However, it is clear from the broader TTBR findings that the Secretary of State will want to rigorously evaluate voting systems until rigor at the national level can be demonstrated. We recommend that the Secretary of State also conduct thorough documentation review as a part of this process so that evaluators have all the material they would need to assess the system.

1.2 Other Key Findings

Key findings not mentioned above include:

- There is a class of attacks against voting systems that has received little to no attention: attacks accomplished by modifying system documentation and procedural documentation. To avoid these kinds of attacks, election officials should have the ability to verify the authenticity of the documents they receive from the Secretary of State and voting system manufacturers. This could involve measures as simple as publishing cryptographic hashes of electronic copies of documents.
- In section 4.1.4, we describe what we call the "leaky pipeline" where problems identified in one part of the certification and elections process may or may not be identified or addressed in subsequent, downstream processes. We propose in the text a few ideas for remedying the leaky pipeline. .
- We were unable to determine if local election officials actually use the *Hart Use Procedures*, as local process and procedures were out of scope for our review. However, Hart operations manuals and other documents provide no state-specific guidance. In this respect, it is crucial that the first answer to California's election officials' questions and issues be the *Hart Use Procedures* document.
- Since Hart sells voting systems in states other than California, their documentation refers to Hart products that are not certified for use in California. However, election officials would only know this by studying the voting system's certification certificate. If these products are packaged with the Hart system, there is a risk that an election official would use a product uncertified for use in California, thereby subjecting the voting system to technical risks and the jurisdiction to legal risks. We recommend that the *Hart Use Procedures* clearly state that these products are uncertified and, as such, should not be used.

2 Introduction: Scope and Methodology

Documentation for a system is intended to enable use of the system both under normal operations and in exceptional circumstances—equipment failures, unpredictable circumstances, etc. With complex systems, procedures for operating the system are a particularly critical component of the overall documentation. For voting systems, the procedures should aim to prevent failures in the election process as a whole despite failures in the technology.

In addition to system documentation and specifications supplied by the voting system manufacturer, another class of important documentary material is the reports of state and national level certification testing. Certification testing at the national level assesses whether or not a voting system complies with the requirements of national voting standards. After national certification, state election officials, ideally, need only gauge how well voting systems meet state-specific standards or standards that are meant to raise the bar above the baseline of national certification. Meticulous documentation performed at both levels of testing is essential for future evaluators to understand what was tested, how it was tested, what the results were and under what conditions the system might not have been tested.

No real methodology for systematic assessment of voting system documentation exists. We therefore developed our own methodology in conjunction with other TTBR Documentation Review teams, adapting it throughout the process. We began with the VSS and reviewed other standards for criteria for assessing documentation. After generating a sample set of frameworks, we used that to inform our development of a framework along the various axes of the election phases; the types of equipment; and the types of documentation (technical specs, user manuals, standards, etc.). We also conducted two walkthroughs of an election, from ballot definition through tabulation of election results. In each walkthrough we sought to conduct an ordinary Election operation relying on the documentation. We also, when practical, engaged in informal "stress testing", pushing the system in ways that seemed like possible modes of human error as we walked through it. We consulted with the Hart Red Team and Source Code Team throughout the Documentation Review process.

In general, we evaluated first the ***completeness*** of the documentation. Here we sought to ensure that we were in possession of all the documentation the vendor intends to be relied upon by election officials as well as documents reviewers would need to understand the system. This included the completeness of the documentation inventory based on references in ITA reports, use procedures, and internal references. We also examined, generally, whether the documentation, as a whole, completely documented the system.

We then evaluated the ***sufficiency*** of the documentation—how well the documentation enabled operation of the system. The documentation covered functional and product specifications; ITA reports; state-level certification reports and data; state-level use procedures; technical support manuals; and user manuals. In addition, we also evaluated to the extent possible (a) suggested or required procedures; (b) system configurations; and (c) system-generated documentation (reports, logs, user interface features). We evaluated this documentation along five critical performance axes, assessing whether the documentation enabled voting officials to perform their duties. We wanted to assess,

from a documentary perspective whether the voting system is (a) usable; (b) accurate and reliable; (c) secure; (d) protective of ballot secrecy; and (e) auditable. In general, we sought to assess the documentation as a whole along these axes, rather than by assessing each piece of documentation separately.

We specifically reviewed each individual document and its role in the election process; compared Hart-generated documentation (including suggested procedures) against the *Hart Use Procedures*[2] (generated iteratively between Hart and the Secretary of State); conducted two brief walkthroughs of the equipment using the documentation; reviewed the adequacy of the documentation and procedures based on the VSS; and reviewed the adequacy of the documentation and procedures based on Source Code Team and Red Team ongoing findings and input.

The Doc Team was based at the University of California, Berkeley, and consisted of two members: a PhD student at the UC Berkeley School of Information, and an attorney and former systems librarian. We reviewed documents from time of receipt on June 6, 2007, through July 13, 2007, and conducted our walkthrough examination of the system documentation on July 3, 2007.

2.1 Limitations

Out of scope of this review was a comprehensive evaluation of the logs produced during normal operation and during test operations. Such a review should be conducted both systematically and forensically. A systematic analysis would include (a) reviewing the logs top-to-bottom for any issues that show up in the logs, and (b) checking to be sure that all known issues are reflected in the logs. A forensic analysis would include a blind test including red team attacks, followed by a review of the logs to identify any attacks and remedy them.

Also out of scope for this review is a thorough evaluation of the user interface of the system. User interfaces, both the user interface available to the voters and available to election officials and pollworkers, can present significant issues relevant to accuracy, security, privacy, and usability. As such, user interface issues are addressed throughout our analysis. We have included comments on the user interface where appropriate, as determined from documentation review and our walkthroughs. However, these comments should not be taken to indicate a thorough review. In particular, the *absence* of commentary on user interface features or default configurations should not be taken to signify that these aspects of the system are optimal or even functional.

For the functions within the scope of our review, there remain significant limitations. First, although we communicated throughout the process with the Hart Red Team and Source Code Review Team, time constraints imposed on all teams prevented us from extensive vetting of the documentation against their final reports and findings.

In addition to the items above listed as out of scope, we stress that our evaluation was more opportunistic than systematic. That is, we followed a rough plan (see section 2) but

[2] *Voting System Use Procedures for California: Hart Voting System 6.2*, California Secretary of State, July 2006, *available at:* http://www.sos.ca.gov/elections/voting_systems/proposed_system6_2_use_procedures_v2_0.pdf.

allowed our instincts to guide us in certain directions that felt promising. Ideally, a systematic study of documentation would involve the following elements:

- Verification of documentation received and acquiring any missing documents needed;
- Full access to a functioning voting system, in order to closely review the usability and accuracy of the documentation;
- Developing a code book of requirements and heuristics from standards, laws, regulation and Secretary of State policy;
- Systematic evaluation of all documents using this code book including methodological checks for inter-coder reliability;
- Organization of this data into themes by code book element;
- Synthesis of each theme into individual theme reports to facilitate a global view of the documentation through the lens of each theme; and,
- A final global synthesis including interactions across themes.

Unfortunately, due to the sheer volume of documentation, time constraints and resource constraints, we quickly determined that systematic thematic coding would not be possible. We hope that something more along these lines will be possible in the future.

3 Hart InterCivic System Description

3.1 Overview of the Hart system

In this section, we give a brief overview of the software and hardware components that make up the Hart system. In following sections, we give detailed descriptions of each.

The Hart system is comprised of a suite of proprietary voting system components running proprietary software, and a Windows-based election management system (the "Hart Election Management System", or "**HEMS**"). Election data is transported from the proprietary hardware to the HEMS on removable PCMCIA memory cards, or optionally transmitted via modem or local network.

The Hart Election Management System is comprised of several different interoperable software modules, coordinated by the Ballot Origination Software System ("**BOSS**"), which jurisdictions use to define an election, burn election media and create an election database. All HEMS software applications run on Windows-based machines.

In setting up the system, the eSlate Cryptographic Module Manager ("**eCM Manager**") is used to generate cryptographic security keys for the system. The security keys are written to a third-party USB security key, which is required for secure functions by BOSS, Tally, Rally, Ballot Now, and SERVO—the Windows-based software applications that comprise the HEMS. **SERVO** is used to service and configure election hardware. Specifically, SERVO is used to configure the devices for the current elections; to archive logs and vote records from the hardware (JBCs, eSlates, eScans); and to clear information about prior elections.

Elections are defined in BOSS, which creates the election database and generates ballot templates. BOSS writes the ballots on the "Mobile Ballot Box" ("**MBB**"), an ATA flash memory card (PCMCIA card). **Ballot Now** is used to print ballots on demand, scan ballots using a commercial scanner, and resolve ambiguous and write-in ballots.

The MBB stores a complete set of all election definitions, as well as the votes and audit logs for any device in which it is used. The MBB is used by the Ballot Now software to print ballots on demand as well as to store vote data created after scanning paper ballots in batches. It is also used to configure proprietary hardware used in the election: the Judge's Booth Controller ("**JBC**") and the **eScan**, both of which record ballots to the MBB.

The JBC connects to and controls up to twelve **eSlate** devices (or up to eleven eSlates and one eSlate DAU). The eSlates/DAUs devices allow a voter with a valid voter access code to activate a ballot, and present an interface to the voter for voting. The units also are connected with the Verifiable Ballot Option ("**VBOx**"), a printer that prints a voter-verified paper audit trail ("**VVPAT**"). When the voter chooses to officially cast the ballot, the voter's votes are recorded on the eSlate or eSlate/DAU, and also transmitted over a local network to the JBC, which records the Cast Vote Record ("**CVR**") on an MBB.

Votes may also be cast using paper ballots, which are scanned with the **eScan** (or a commercial scanner attached to the Ballot Now computer). The eScan, like the JBC, draws ballot information from an MBB. The eScan scans paper ballots, creating a CVR for each ballot, which it records to the MBB.[3]

When the election is closed, the MBBs may be taken back to Election Headquarters and read by **Tally**, or taken to distributed stations and read by a workstation running **Rally**. Results read in Rally are transmitted over a local network or via modem to a server running Tally for unofficial early tabulation. Regardless of whether Rally is used, the MBBs will ultimately be taken to Election Headquarters.[4] The Tally program is used to tabulate election results and to produce reports based on the election database. It tabulates the unofficial results from the CVRs transmitted by Rally, and directly from the MBBs using a USB PCMCIA card reader. Results may be manually adjusted in Tally as part of the final Canvass.

The **SERVO** program is used to reset the eScan, eSlate, and JBC devices, zeroing them out for use in new elections, copying the cryptographic signing key to them, and (optionally) archiving their contents. SERVO can be used to create a "recount MBB" which can be used to verify the Tally results generated directly from the MBBs and/or based on Rally tabulations.[5]

All the Hart EMS software programs run on Windows 2000 Professional, with Service Packs 3 and 4 variously specified throughout the documentation.

---

[3] *Hart InterCivic Software Qualification Test Report,* CIBER Labs, NASED Number N-1-04-22-22-006 (2006), Section 4, pp.8-9.
[4] *Hart Use Procedures*, note 2, page 49.
[5] *Id.*

3.2 Component Details

3.2.1 eCM and eCM Manager

The eCM is a USB device manufactured by Spyrus, Inc. and provided by Hart. It is used to secure access to the Windows-based machines running the Hart EMS. It includes the cryptographic signing key, which is generated by and written to the eCM by the eCM Manager. One or several eCMs may be created for any one election; all will include the same key and hash information, but may have different PINs. eCMs may be reused from election to election, but a new election-signing key should be created for each election. The system overwrites old data.

The eCM Manager ("eSlate Cryptographic Module Manager") is a software program, part of the Hart Election Management System (HEMS). It is used to write (and verify) a **Key ID**, a **Key GUID** (key globally unique identifier), a **signing key**, and a **hash** to an eCM. A password (called a "PIN" in the documentation)[6] is required for each eCM. The PIN is a 6 to 12 character, case-sensitive password.

The Key ID is an integer from 0-99 that is specific to the election and provided by the user. The system does not require the key ID to be unique from election to election; it is effectively a label for the uniquely generated signing key (also called the "election signing key"). When a new key ID is entered, the system generates a secret signing key,[7] a 128-bit random number. The Key GUID is a unique system-generated value assigned to each signing key. When the user enters a "PIN" during the configuration process, the eCM Manager writes to the eCM the key ID, key GUID, signing key, and a hash to verify the keys.

The documentation recommends writing down the "PIN" (password), Key ID, and Key GUID for all eCMs, and maintaining that in a "secure location".[8] The documentation also recommends storing an electronic copy of the keys as an ".eCM" file in a "separate location (e.g., the local PC drive or a CD)."[9]

The various software applications use the eCM key information to access sensitive functions, including writing election media (the MBBs), formatting election hardware (eScans, JBCs), and tabulating election results. By writing the keys to the various hardware and software applications, the MBBs and hardware are required to validate each other, and the Rally/Tally applications are required to validate the MBBs before tabulating election results. Each time a new key is generated, each piece of hardware (JBCs, eSlates, and eScans) has to be processed in SERVO with the new keys.

The eCM Manager software apparently has no audit logging capability.

---

[6] Throughout the Hart system documentation, there is confusion between the terms "PIN" and "password". A "PIN" ("personally identifiable number") is a numeric code, and a password can include alphanumeric characters. This is a minor but unnecessary confusion in language.

[7] *Hart Voting System Management and Tasks Training Manual Revision 62A* ("*Management & Tasks*"), Hart InterCivic, Inc., Part No. 6300-001, May 2006, p.42.

[8] *eCM Manager Operations Manual*, Chapter 2: Write New eCMs, p.27.

[9] *Id.*

Versions: Version 1.1.7 is certified in California as part of Hart System 6.2.1.[10] It was originally certified on March 10, 2006, for use in California as part of Hart System 6.1 and was included unchanged in System 6.2.[11,12]

3.2.2 BOSS

BOSS ("Ballot Origination Software System") is the Hart EMS program that creates an election database for the election, generates ballot styles and formats, and writes the MBBs.[13]

BOSS, like all other parts of the Hart EMS, runs on Windows 2000 Professional; both Service Packs 3 and 4 were specified throughout the documentation. BOSS also requires a third-party database for the election; although not specified in the user documentations, the TTBR configuration included a Sybase database. BOSS also requires third-party software (unspecified) for print previews.

Access to secure functions in BOSS is managed with an eCM and the eCM "PIN".

BOSS includes basic report functionality for most portions of the election database, and generates an audit trail report which is stored on the BOSS machine. The BOSS audit trail generally tracks add, delete, and update actions to the portions of the BOSS database (e.g., ballot templates, instruction test, party information, proposition text).

Versions: Version 4.3.13 of BOSS is certified in California.

3.2.3 MBB

The MBB ("Mobile Ballot Box") is a flash memory card used to store the ballot definitions and the voted ballots (the "Cast Vote Records", or CVRs). MBBs each have a unique serial number, which is used by Tally to prevent the same MBB from being read twice during tabulation.

MBBs are created in BOSS. BOSS may create standard MBBs (for use in JBCs, eSlates running in SOLO mode, DAUs, eScans, and machines running Ballot Now); test MBBs (for use in acceptance testing, functionality testing, logic and accuracy testing, etc.); or demonstration MBBs (for use in demonstration eSlates). Demonstration MBBs include ballot templates and audio recordings, but do not record CVRs. After BOSS creates an MBB, the MBB may initially be read by any Hart election device or program. Once installed in a machine and read, however, it is initialized for that machine and may not be used in a different machine.

This standard PCMCIA card may be used to create either MBBs or audio cards. The audio cards carry audio recordings of relevant ballots, and are created in BOSS. These cards are inserted in an eSlate DAU. The Hart EMS recognizes audio cards as such and

---

[10] *Approval of Use of Hart InterCivic System 6.2.1 DRE and Optical Scan Voting System*, California Secretary of State, September 22, 2006, *available at:* http://www.sos.ca.gov/elections/voting_systems/2006-09-22_System_6_2_1.pdf.

[11] *Id.*

[12] *eCM Manager Operations Manual Revision 11-60B*, Hart InterCivic, Inc., Part No. 6100-080, November 2005.

[13] *Hart Voting System Ballot Origination Software System Operations Manual Revision 43-62B*, Hart InterCivic, Inc., Part No. 6100-019, May 2006 ("*BOSS Operations Manual*").

will not record CVRs on them.

Once the BOSS database is finalized for use with Tally, no further MBBs may be created. Documentation advises elections officials to create 10% more MBBs than the number needed in case of failures, unanticipated needs, etc.[14]

Three major types of data are stored on MBBs: (1) The ballot definitions and polling place IDs; (2) the cast vote records (CVRs); and (3) the audit logs for the device. MBBs apparently come in capacities of 128MB, 256MB, etc.[15] A standard 128-MB MBB capacity card can hold up to 10,000 JBC CVRs; 65,000 Ballot Now CVRs; 20,000 eScan CVRs; or 65,000 SERVO CVRs, in addition to audit logs and ballot definitions.[16] Audit logs show that some programs generate disk space warnings.

3.2.4 Ballot Now

Ballot Now is Hart's software for printing paper ballots on-demand and scanning in and resolving batches of voted paper ballots.

Ballot Now, like other applications in the Hart EMS suite of software, runs on a Windows 2000 Professional machine. It works with a variety of third-party scanners.

Ballot Now can be run on a stand-alone machine or in a networked, client/server configuration. Users must configure network certificates to run Ballot Now in a networked configuration.[17] If run in networked configuration, the eCM must be present on the Ballot Now server. If run in standalone configuration, the eCM must be present on the standalone Ballot Now machine.

After defining an election database in BOSS, Ballot Now initializes an election MBB and creates a Ballot Now election database (stored in a unique folder for that election, in the file "ballotNow.db"). Ballot Now's central features are (1) to print sample, test, and election ballots, either for third-party printing or on demand; and (2) to scan paper ballots (using the "Ballot Now Image Processor", or BNIP); and (3) resolve undervoted, overvoted, and/or write-in contests. Results from scanned and resolved ballots are written to an election MBB, and after processing is done, the Ballot Now user closes the MBB using a "close MBB" function in the software.

Ballot Now produces several types of audit logs—the Election Database Audit Log; the Security Database Audit Log; the Filtered Election Database Audit Log; and the Filtered Security Database Audit Log.[18]

Version: version 3.3.11 is certified in California.

---

[14] "Planning Ballot Media Quantities", *Management & Tasks*, note 7, p.27 (PDF p.33).
[15] *Management & Tasks,* note 7, p.27 (PDF p.33); *see also Hart InterCivic online catalogue approved by Texas Building and Procurement Commission*, Hart InterCivic, Inc., *available at:* http://www.hartic.com/innerpage.php?pageid=55.
[16] *Management & Tasks*, note 7, p.28 (PDF p.34).
[17] *Hart Voting System Ballot Now Operations Manual Revision 33-62B*, Hart InterCivic, Inc., Part No. 6100-067, p.25; p.37; p.40; p.246-247 ("*Ballot Now Operations Manual*").
[18] *Id., Ballot Now Operations Manual*, p.25; pp.219-232.

3.2.5 SERVO

SERVO ("System for Electronic Records and Verification of Operations") is a program that backs up CVRs and audit logs from voting devices. It also resets voting devices (eSlates, eScans, JBCs) for use in new elections. SERVO may also be used in recounts and audits, since it accesses and archives data directly from the voting devices. SERVO is a back-office application; it is intended to be used in the storage warehouse before and after deploying the equipment. SERVO is installed by Hart personnel, and may be run on one or multiple workstations.

Each device connects to SERVO using a different type of connection. The eScan connects to the SERVO using a network crossover cable on the ethernet ports. The JBC uses parallel cables. The eSlates are connected to the JBC with a "JBC-to-eSlate" cable, which is a proprietary serial cable.

When each device is connected to the SERVO machine, the SERVO program writes the election key (which has gone from eCM Manager, to eCM, to SERVO) to the JBCs and eScans. The Functional Specifications note that SERVO also writes the signing key to the Demonstration eSlates.

SERVO erases CVRs from prior elections, erases the internal audit logs, and sets the clock on all devices and configures the election key information into the hardware (JBCs and eScans).[19] SERVO resets the public counter, but not the private counter on each device. The private counter in JBCs and eScans thus constitutes a usage record that records the number of ballots cast on each device.

SERVO is also used in recounts and audits. As it reads the JBCs, eSlates, and eScans, it can generate recount data from the CVRs stored on those devices; that recount data may be compared with the data transmitted via the MBBs to Tally. For a recount, SERVO writes to one or more unused BOSS MBBs all CVRs from every JBC, eSlate, or eScan backed up for a given Election Event.

SERVO can also "reconstruct" MBBs from its backup copies of the election device internal memory and audit logs (but not, apparently, directly from the equipment[20]). Device-level copies of CVRs are generated when the voter casts the ballot, and may therefore be used to compare with the MBBs, and to detect tampering with the election media that occurs *after* the ballot is cast. (However, they would not be helpful in detecting interferences earlier in the process.) When reconstructing an MBB from an eScan or JBC, the memory of a single device is written to a single MBB.

eSlates are wiped clean by SERVO (public count reset and memories erased), but they do not generally receive any other election-specific configuration information. Instead, eSlates are generally run by software on the JBC.

SERVO may be installed on multiple workstations, with one workstation designated as a "Master SERVO" machine. The partial files from each individual SERVO workstation are copied manually to the Master SERVO database directory using Windows file

---

[19] Election officials set the time and daylight savings time settings on SERVO, which then programs time into all the election devices.

[20] *See: SERVO Functional Specification*, listing this as a "Future Enhancement." *SERVO Functional Specification*, Revision 42-62B, Hart InterCivic Inc., April 10, 2006, Part No. 6000-099.

manager; an internal SERVO software process ("Import Device Data") is used to identify and consolidate the files into a master database.

SERVO stores major user actions to an internal audit log, including login, backing up devices, creating recount and recovery MBBs, firmware validation, and data imports.

Versions: version 4.2.10 is certified in California.

3.2.6 JBC

The JBC ("Judge's Booth Controller") is a console device that controls up to 12 eSlates, or one eSlate DAU and up to eleven eSlates over a local network. The pollworker uses the JBC to open the polls, close the polls, print access codes for voters to use with the eSlates, print zero and totals reports, and store CVRs on the JBC and the MBB.

The JBC is networked to the eSlate terminals, which are daisy-chained via serial cable. The JBC hardware comes in at least two configurations. The JBC 1000B includes a modem port for connecting to voter registration databases using an unidentified voter registration product, which has not been certified for use in California.[21] The JBC 1000 does not include a modem port.

The JBC interfaces with a MBB to get ballot information, which it uses to send ballots to the connected eSlates. The pollworker requests the JBC to print an access code on a small piece of thermal paper; the user then takes that access code to the eSlate, enters it, and the JBC sends an appropriate ballot to the user. Ballots may differ by party, for instance, or even precinct in a split precinct.

If the JBC blows a fuse, or presumably if it loses power at all, the troubleshooting manual states that it may, or may not, print an "Aborted Access Codes" report. This report can be used to verify the status of a voter's access code, which may need to be reassigned if the voter's code has been aborted or deactivated.[22]

When the user casts the vote and approves the VVPAT, the CVR, or image of the ballot choices, is transmitted back to the JBC and written to the MBB. The JBC also stores copies of the CVRs on its local flash memory.

The JBC can print an unofficial tabulation when polls open and close. When polls open the JBC prints a zero report that should show that all contests have zero ballots case. When polls close, the JBC prints a totals report that itemizes votes cast per choice per contest.[23] The totals report is required to be posted at each polling place in California.[24]

Versions:

- Hardware models: JBC 1000B v. JBC 1000
- Software version: 4.2.13

---

[21] According to Proebstel et al, (note 66, *infra*.) the JBC 1000B is in use in at least one California county.
[22] *Hart Voting System Support Procedures Training Manual Revision 62C*, Hart InterCivic, Inc., Part No. 6300-006, p.152 (PDF p.158) ("*System Support Procedures*").
[23] This is a configurable option that must be specified in BOSS.
[24] California Election Code, ("CA Elec. Code") section 19370.

3.2.7 eSlate and DAU

The eSlate is a proprietary hardware device that presents the ballot to the voter, mediates interaction with the voter, and records the voter's selections. It stores the CVR locally in non-volatile flash memory and also transmits it to the JBC. The JBC serial cable provides power, although a battery pack provides power in case of a power outage. Up to twelve eSlates are connected to a JBC by daisy chain.

Although not approved for use in California, the eSlate has the capability to have the last device in the chain removed and taken to a voter for curbside use.

A demonstration eSlate may also be set up, using a demonstration MBB. The eSlate appears to also be capable of running in "SOLO" mode, using an MBB but no JBC (a DAU5000). This configuration does not appear to be certified for use in California

The eSlate can also be adapted to run in an accessible mode, called a DAU. The eSlate DAU has the eSlate functionality, but with different hardware inputs and a PCMCIA card storing locally recorded ballot information for audio output. The eSlate can take input from jelly switches or a sip-and-puff device. It can output the ballot through an audio recording for use with headphones. There is some evidence that the eSlate DAU should be the last eSlate on a daisy chain.[25]

In addition to transmitting the CVRs to the JBC, the eSlate maintains a copy of each CVR locally in non-volatile flash memory. ESlate options are defined in BOSS when the election is defined.[26] For instance, the ability to disable the unique ballot ID for early voters and whether or not to include a Ballot Key (serial number) for each ballot is configured during BOSS election definition.

Versions: version 4.2.13 is certified in California.

3.2.8 VBO

The VBO ("Verified Ballot Option") is used to describe an eSlate voting booth that contains an eSlate and the VBOx, a sealed voter-verified paper audit trail (VVPAT) printing unit with a window through which voters may verify their VVPAT. The VBOx is a small printer using thermal paper—similar to a cash-register receipt printer, but about 4" in width. The printer stores the printout on a reel and scrolls the printout for review. After the voter reviews a ballot on the printout, accepting the ballot advances the paper to ensure that the last voter's choices are not visible to the next voter. Canceling the ballot or changing the contents prints a voided status notice below the ballot. After the voter has changed her ballot and selected "cast ballot", another ballot is printed for review and a barcode is written with the message "ballot accepted". If the voter cancels their ballot more than the maximum number of permitted cancellations, the system forces the last ballot and VVPAT to be recorded. VVPATs that span multiple pages require the voter to inspect each page before scrolling to reveal subsequent pages.

---

[25] *Id.,* The *Support Procedures Training Manual*, PDF p.48, shows DAUs at end of the eSlate daisy chain in a figure entitled "eSlate System Acceptance and Functionality Test Workflow"; *see also* "Planning Polling Place Layout" in the *System Support Procedures*, note 22, pp.87-88 (PDF pp.93-94).
[26] *BOSS Operations Manual*, note 13, pp.118-125.

The VBOx is listed as requiring a separate, dedicated power cord instead of receiving power over the serial cable. However, in the pre-election setup, the jurisdiction is advised to install batteries—a 6-alkaline battery pack. It is unclear whether the device is battery-powered or electrically powered. Testing by the TTBR Hart Red team suggests that, with the model VBOx provided for review, if either the VBOx or eSlate lose power the corresponding device ceases to work.

The VBO prints both human-readable text and machine-readable barcode. The barcode is a standard two-dimensional barcode that encodes the contents of the VVPAT and basic information about the election in which the vote was cast and the machine on which the ballot was cast. The Hart VVPAT can be configured with a serial number (called a "Ballot Key") in order to detect duplicate ballots. In California, identifying information at the individual ballot level, such as the Ballot Key, is not permitted.[27] The Ballot Key feature is configurable during ballot definition in BOSS, and in California, must be disabled.[28]

Versions: version 1.8.3 is certified for use in California.

3.2.9 eScan

The eScan is an optical scanner ("op-scan") unit used to scan paper ballots. The eScan is a dedicated proprietary piece of hardware, with a built-in automatic feed scanner, a thermal line printer, local flash memory, and two secure compartments for ballot storage.

The eScan is intended to be used only with ballots printed in advance on paper of a specified weight and dimension. Voters or pollworkers feed the ballots into the eScan one at a time. The eScan scans the ballots, creates a CVR from the ballot (including images of any written-in candidates), and stores the paper ballot in one of the two ballot storage bins (a scanner bin and a bin for use in emergencies that has an access slot). The CVR is written to an MBB.

The two ballot storage bins are each sealed with a Hart security seal at election headquarters, and the emergency ballot slot is opened to allow depositing of paper ballots during emergencies (such as power failures) without disturbing the security seal on the ballot bin door. Jurisdictions can choose to seal the MBB into its compartment before delivery of the equipment to the polling place; alternatively, they can deliver MBBs to polling places on election day morning and seal them then.

eScan options are defined in BOSS when the election is defined.[29] The eScan unit itself maintains audit logs that include system startup and shutdown information, CVRs written and other events like ballot rejection overrides.

The eScan units are configured by SERVO, which resets the time, public counter, CVRs, signing key, and audit log. SERVO also optionally resets MBBs in the eScan to clear the

[27] *California Elections Code* § 15208 ("Any ballot that is marked in a manner so as to identify the voter shall be marked "Void" and shall be placed in the container for void ballots."). The California Secretary of State on May 18, 2006, issued the *Uniform Vote Counting Standards*, which further elaborates the markings that a voter might make that would render a ballot void, although it doesn't address markings that voting equipment might make.
[28] *Hart User Procedures*, note 2, pp.10, 15.
[29] *BOSS Operations Manual*, note 13, pp.126-134.

CVRs and audit logs. SERVO can also back up CVRs and audit logs from the eScan, and create a Recovery MBB from those records.

Versions: version 1.3.14 is certified for use in California.

3.2.10 Rally

Rally is one of the back-end software programs in the Hart InterCivic Election Management System. Rally operates as an intermediate step between voting and final tabulation. It is intended to operate in a distributed fashion, at secure facilities designated as "Rally Stations", providing early "unofficial" election results. JBCs and eScans containing MBBs may be brought to the Rally centers and read by the Rally stations, which copies the data off the MBBs in the same fashion that Tally does. Tally polls the Rally stations periodically (at a regular period of time designated during setup by an election official; every 15, 30, or 60 minutes[30]). The Tally-Rally connection is initiated by Tally, and transmits election results in aggregate via a modem or ethernet connection, using SSL ("secure sockets layer").

Versions: version 2.3.7 is certified in California, although it is unclear whether any jurisdictions actually use it.[31]

3.2.11 Tally

Tally is the software program component of the Hart Election Management System that reads and tabulates CVRs from MBBs.

Tally is secured with the physical USB key and password protection. The Tally database is initially created with an MBB from BOSS. After the Tally database is initialized, and prior to beginning tabulation, Tally requires input of any approved write-in names.

When polling places are closed, the MBBs are returned to election headquarters, and Tally copies the data stored on all the MBBs. This includes MBBs from Early Voting and Election Day, whether stored on JBC MBBs, eScan MBBs, or Ballot Now MBBs. Tally also copies the audit trail, which is stored on the MBBs with the CVRs. Tally uses the MBB's unique serial number to prevent reading the same MBB twice during tabulation. Provisional ballots and write-ins are resolved using Ballot Now, which also produces an MBB for use with Tally. Tally also permits vote adjustments by elections officials. When all MBBs have been read by Tally, the database is Finalized and archived.

---

[30] *Tally Operations Manual,* Chapter 3 "Election Information", "Transferring Vote Counts from Rally", p.83.

[31] CA Elec. Code §19250(g) says "A direct recording electronic voting system shall not be permitted to receive or transmit official election results through an exterior communication network, including the public telephone system." It is unclear how this might apply to the Rally-Tally transaction. It appears that Rally sends an aggregation—a tabulation—of the information from the MBB to Tally. See, e.g., *Rally Operations Manual*, "How Rally Works", p.18 ("Tally … connects to the Rally station and downloads the ballot counts into the Tally Election database"). This may, or may not, constitute a "result". It also may, or may not, be "official"; while Tally generates the official final result, the Rally aggregate of the MBB may also constitute an official result for that precinct, or MBB. Finally, there is a question of whether Tally's sending of the results constitutes a "DRE" sending the results.

Tally's database includes all CVR and audit trail information from all MBBs read by Tally, and can thus be archived as a complete record of the election. This is not the case when Tally is used in conjunction with the early election return program, *Rally*. When Tally-Rally operations are enabled, Rally reads the MBBs, and Tally polls Rally for the summary results. Rally maintains its own election database of MBBs read in Rally, and the Tally election database does not include that information.

Tally includes extensive reporting features. Among the tracking and auditing features, Tally tracks which MBBs have been returned (using the BOSS data about MBB generation). Tally reports and logs may also be verified against SERVO logs generated directly from election devices (JBCs, eSlates, and eScans). Election data may be exported in tab-delimited or EDX ("Election Definition XML") file formats.

Versions: version 4.3.10 is certified in California.

4 Completeness of Documentation

The documentation we received generally consisted of materials that the California Secretary of State receives from the vendor as part of the vendor's California certification application materials:

- ITA reports and correspondence – These documents consist of reports and correspondence from the Independent Testing Authorities that conducted national certification testing. These are proprietary documents, intended for use by national and state certification authorities.
- State-level certification reports and data – These reports give a high-level report on what testing was performed at the state-level and include data from volume testing. These are public documents.[32]
- Use Procedures – California requires each vendor to adapt its procedural documentation specifically for California law and regulation. The Use Procedures document is a public document intended for election officials that contextualizes the system documentation and procedures within California-specific requirements.
- Technical specifications – These documents are internal Hart functional and product requirements documents that describe what the product is functionally capable of and the high-level requirements for each product. These documents are proprietary and confidential, and are intended for use by vendor employees and provision to certifying authorities.
- Operation manuals, training manuals and pollworker documentation – These documents are the users manuals, support manuals and training materials that customers receive. These allow the customer to operate their voting system, maintain it and train other staff to work with it. These items are largely classed as proprietary documents.[33] They are intended for use by "users" of the vendor

[32] The Secretary of State identified some of these documents as proprietary.
[33] Arguably, many of these—such as poll worker user manuals—contain no trade secrets.

system: election officials, poll workers, and technical support staff that provide assistance to election officials.

4.1 General Comments

4.1.1 Missing documentation

In a number of instances, documents that we knew existed were unavailable.[34] Documents we did have referenced other documents that were not provided to us. In order to identify missing documents we examined the list of documents provided to the ITA laboratories and examined references to documents within available documents. The following sections itemize documents we did not originally have available for our review.

4.1.1.1 Missing Hardware ITA report

When we began our review, we were not in possession of the Wyle Hardware ITA report for system 6.0.[35] We had only letters from Wyle that specified nothing had affected the hardware qualification after system 6.0. We requested this document from the Secretary of State and were provided with it after our review had begun. We were unable to determine if the State or its consultants had access to this report previously.

4.1.1.2 Missing Training Manuals

We were missing a number of training manuals:

- BOSS training manual, Part No. 6300-002 62A
- Ballot Now training manual, Part No. 6300-003 62A
- Tally training manual, Part No. 6300-005 62A
- Rally training manual, Part No. 6300-005
- Train the Trainer Handbook, Part No. 6300-008
- eSlate PVS DAU 5000 Voting Unit Setup, Part No. 6000-057
- Ballot Now Voter Instruction, Part No. 6300-700
- eSlate Voter Instruction Script, Part No. 6300-400

These documents were internally referenced, both in the *Hart Use Procedures* and in the *Management and Tasks Training Manual*.[36] The references indicate that these documents include procedures and other information that elections officials would rely upon in setting up the system or instructing poll workers or voters in its use. Because these documents were not provided to us, issues that we describe may be covered by and/or remedied by these documents.

[34] Note that some missing documents, such as ITA test plans, have never been available to reviewers.
[35] *Wyle Hardware ITA Report*, note 61.
[36] *Id.*, note 7.

4.1.1.3 Other Missing Documents

For most Hart products, we have a functional specification and a product specification. However, each of these documents also includes a section entitled "References" where all other documents referenced are collected. By examining these lists and eliminating documents we did have, we were able to determine we did not have the following documents:

- Quality Manual, Part No. 6000-003
- eSlate Design Specification, Part No. 6000-006
- JBC Design Specification, Part No. 6000-008
- Hart PVS Communication Specification Document, Part No. 6000-009
- PVS Audit Log Specification Document, Part No. 6000-011
- MBB Requirements Specification, Part No. 6000-012
- Rally Functional Security Specification, Part No. 6000-106
- Tally Functional Security Specification, Part No. 6000-107
- Servo Functional Security Specification, Part No. 6000-139
- Ballot Now Security Functional Specification, Part No. 6000-140
- System Security Requirements, Part No. 6000-166
- System Security Functional Specification, Core Products, Part No. 6000-174
- PVS Security Functional Specification Document, Part No. 6000-183
- VBO Functional Security Specification, Part No. 6000-189
- eScan Security Functional Specification, Part No. 6000-196
- eCM Manager Functional Security Specification, Part No. 6000-243
- HVS Polling Place Report Functional Specification, Part No. 6000-296
- Printer interface PCA, Part No. 2001-660

We are unable to determine how access to these documents might have changed the result of the TTBR analysis or our document review.

4.1.2 System Versions

The Hart system under review was system 6.2.1. The previously certified version was version 6.1. The largest difference between these two versions was the ability to turn off ballot serial numbers during election definition, required by California. While system 6.2 was initially submitted for certification, an anomaly in the JBC component with respect to printing totals tapes of consolidated precincts necessitated a JBC firmware change that was then recertified at both the national and state levels.[37]

[37] Lack of definition or specification of particular versions of hardware was particularly noticeable. Particularly when hardware includes both version numbers for the hardware itself and for the software that

4.1.3 Document Versioning

Hart's documents contain clear versioning information, both of the document and the version of software/hardware documented.

There was some variation in the specification of Windows 2000 Professional. For instance, the Hart Voting System Product Description[38] specifies Service Pack 3 (pp.40-42), while the CIBER ITA report specifies Service Pack 4 (page 5).[39] This should be rectified in the documentation.

However without other versions of the documents, it is difficult to verify the accuracy of the version references and to evaluate whether changes made to versions have been adequately described. It is also difficult to track the many documents through different hardware/software changes.

We recommend that creation and maintenance of a comprehensive changelog index for all documentation. Each document should be indexed in the changelog, and significant changes should be described and given version numbers. The index should include hashes for these documents. Numerous programs track versioning of documents now, and many documents include a changelog. These features would facilitate certification and review of the documentation of the election system. Since procedures for maintaining the integrity of elections are specified in the documentation, this constitutes an integral part of the overall election system. Understanding changes to these procedures is critical for assessing the election system.

4.1.4 The Leaky Pipeline

One problem with documentation that we observed may be called the "leaky pipeline", which manifests as problems that are noticed at some point in the certification, review, and implementation process, but are never fully addressed.

During the course of state certification reviews and during elections, problems were flagged in the error logs but did not make it into the certification report. Problems that did make it into the certification report, stated explicitly as recommendations for the *Hart Use Procedures*, did not always make it into the Use Procedures document. Problems that made it into the Hart Use Procedures did not always make it back into the Hart documentation, which includes the detailed checklists and logs and step-by-step procedures that users are likely to be actually following. Finally, of course, even procedures that make it into the Hart documentation may be missed in local implementations and actual practice.

This problem—a sort of "leaky pipeline" of recommended procedures and system issues—can undermine the effectiveness of the numerous measures put into place around equipment. For this reason, effective indexing and crosschecking of prior review findings should be implemented as part of downstream review procedures themselves. For example, the ITAs could index each event, and separately describe the outcome:

---

it runs—as in the JBC—elections officials who are given only one of the two kinds of version information may be unaware that there are other relevant versioning information.

[38] *Hart Voting System Product Description Revision 62A*, Hart InterCivic, Inc., Part No. 6000-060 ("*Hart Product Description*").

[39] *Id*, note 3.

"resolved"; "deemed minor"; "recommendation #1". Each item that results in a recommendation from either the ITA or state consultants would comprise a checklist that the Secretary of State should use in developing a supplement to the *Hart Use Procedures*. This way, each item identified would be incorporated in a checklist that would be used at the next step along the pipeline, effectively "plugging leaks".

4.2 User Documentation

Hart's user documentation included

- Operations Manuals for the six individual major software components, plus a "product description" that describes the system as a whole;
- Training manuals for the major software components were referenced but not included;
- *Hart Voting System Management and Tasks Training Manual* ("*Management & Tasks*");[40]
- *Hart Voting System Support Procedures Training Manual* ("*Support Procedures*");
- *Voting System Use Procedures for California: Hart Voting System 6.2* ("*Hart UseProcedures*");
- eSlate Early Voting Desk Reference;
- eSlate Election Day Desk Reference;
- Security Procedures (a four-page security procedure taken from Hart Use Procedures);
- No manuals for hardware components, and;
- Little information about Windows configuration issues.[41]

While Hart's documentation is thorough, good short overviews are lacking, or hard to find. The *Management and Tasks Training Manual* ("*Management & Tasks*") is perhaps one of the most helpful documents for the election official, but the useful procedures were scattered across two documents that do not seem to be designed for a similar audience: the *Management & Tasks Training Manual* and the *System Support Procedures Training Manual* ("*System Support Procedures*"). The software Operations Manuals do not provide generally references back to relevant procedures in these two documents.

The *Voting System Use Procedures for California: Hart Voting System 6.2* ("*Hart Use Procedures*"), developed from a standard template that the California Secretary of State provides,[42] is an important overview, and includes some information not included elsewhere (such as the list of Windows networking features that must be disabled).

---

[40] *See Management & Tasks*, note 7.

[41] Section 10.2 of the *Hart Use Procedures* contains some basic information on configuring the HEMS computers, running Windows, but it is probably not detailed enough to allow itemized, comprehensive configuration.

[42] *Voting System Use Procedures for California Template*, California Secretary of State, 2006, *available at:* http://www.sos.ca.gov/elections/voting_systems/use_procedures_2006.pdf.

Election officials in California are required to follow the *Hart Use Procedures* to operate their system[43] although it is unclear how many do. However, they are not sufficiently detailed to be of use in running an election. Paradoxically, the thoroughness of Hart's documentation discourages use of the *Hart Use Procedures*. Hart includes detailed checklists for procedures in *Management & Tasks* and *System Support Procedures*, which encourage elections officials to use those forms and checklists. Unfortunately, the *Hart Use Procedures* contain information not incorporated into the forms and checklists. The lack of integration makes it difficult to clearly understand and follow procedures, and complete important tasks and configurations. We recommend that future Hart documents either incorporate features from the *Hart Use Procedures* (for instance, a "local requirements section" in each form), or at a minimum incorporate flexibility (blank steps in the procedure and checklist forms) that election officials can use to add the steps themselves.

For polling place workers, the *Early Voting Desk Reference* and the *Election Day Desk Reference* are adequate for completing basic tasks. However, they are inadequate for troubleshooting.

In all cases, useful information about dealing with systems is scattered across multiple documents, and indexing to the various places could be improved. In our walkthroughs, the documentation was sometimes confusing as it used a thicket of back-and-forth references. For instance, an election official user creates an election in BOSS, defining the precincts, numbers of voters, and so on. When the user begins to add in candidates, the *Hart Voting System: Ballet Origination Software System Operations Manual, Software V. 4.3* ("*BOSS Operations Manual*") refers the user to "edit active contest", and must follow "see" references from page 200, to page 290, to page 260. A comprehensive subject index including all documents would significantly increase the usability of the documentation.

This exposes a deeper problem with referential integrity of the documentation. Often, Hart documents will refer extensively to other documents to instruct the user where treatment of particular issues is addressed. However, this is problematic when the user might not have the document referred to. This is especially acute in the *Hart Use Procedures*. The *Hart Use Procedures* is a public document partially intended to give the public an idea of how a voting system should be operated in California. However, when this document refers to another document, possibly proprietary or otherwise unavailable, it leaves large holes in the public record with respect to procedures. We recommend that *Hart Use Procedures* minimize references to proprietary or non-public documentation.

The features for TRANS, Fusion, Infusion, and Bravo—all Hart software programs that have not been certified for use in California—are referenced throughout the documentation. For instance, TRANS ("Translation, Recording, and Audio

[43] *See* Memo from Bruce McDannold to All County Clerks/Registrars of Voters/Vendors (CCROV 06373), *Re: Voting System Security Precautions for November 7, 2006 General Election*, October, 25, 2006. This memo, which doesn't appear to be public, describes the status of the Use Procedures for each voting system, "The official Use Procedures and the security requirements set forth in the actual certification document for each system are not optional. They specify important measures to protect voting systems and the integrity of the vote count from known vulnerabilities. […]".

Normalization System"),[44] an application for translating foreign language text and recording audio for import into BOSS, has not been approved despite being referenced extensively in the BOSS Operations Manual.The failure to update documentation to reflect this may be confusing for users. However, of even greater concern is the possibility that, in addition to the user documentation, the security procedures and protocols have not been updated to reflect the absence of these products.

Although we were not in a position to fully evaluate the user interface and system configuration, in evaluating documentation and procedures, some aspects of user interface and system configuration presented issues. These will be discussed in the phase-based portion of the analysis in section 5.1.

4.3 Technical Data Package

The Technical Data Packages ("TDPs") as defined in the VSS include a variety of documents that would have been useful in our analysis. The VSS describes the TDP as:

> "The FEC requirements state that at a minimum, the TDP shall contain the following documentation: **system configuration overview; system functionality description; system hardware specifications;** software design and specifications; system test and verification specifications; system security specifications; **user/system operations procedures; system maintenance procedures; personnel deployment and training requirements**; configuration management plan; quality assurance program; and system change notes."[45]

The items from the TDP that we had available are highlighted in bold text above.

4.4 Laws, Regulations and Standards

The Document Review team also referred to a number of laws, regulations, standards, and publicly accessible documents, including:

- The California Elections Code and related regulations in the California Code of Regulations, title 2, division 7; and the California Government Code.[46]
- The California Voting System Requirements, issued by the Secretary of State in October 2005.[47]
- The 2002 Voting System Standards ("VSS").[48]
- The Voting System Use Procedures for California Template.[49]

---

[44] *Hart Use Procedures*, note 2, p.8.
[45] CIBER, *Hart InterCivic Software Qualification Test Report*, NASED Number N-1-04-22-22-006 (2006), Section 5, pp.10.
[46] California Law is available on the web here: http://leginfo.ca.gov/calaw.html. The California Code of Regulations is available here: http://ccr.oal.ca.gov/linkedslice/default.asp?SP=CCR-1000&Action=Welcome.
[47] *Voting System Requirements*, California Secretary of State, October 2005, *available at:* http://www.sos.ca.gov/elections/voting_systems/requirements.pdf.
[48] VSS, note 1.
[49] *Id.*, note 42.

4.5 Hardware Documentation

In general, hardware specifications were poorly documented in the documents we received. Critical features of hardware are buried in the software documentation for those features, and may be poorly addressed.

4.5.1 JBC Varieties

The JBC comes in two varieties, one with a modem (JBC 1000B; sometimes spelled JBC 1000 B) and one without (JBC 1000). This is referenced in only three places—the *SERVO Operations Manual* (p.31)[50]; a System 6 preliminary Wyle certification test report; and the Battery Pack Test Procedures in the *System Support Procedures*. The Hart VS Product Description specifies the JBC 1000. All other Hart documentation appears to reference the JBC generically. The 1000 B is apparently intended to support the Hart products for voter registration databases, which have not been certified for use in California. However, these features are discussed throughout the documentation. The JBC 1000B modem connection presents significant security and confidentiality issues[51] that the JBC 1000 does not, and election officials should be fully informed of both varieties.

4.5.2 EScan "Emergency Ballot" Features

Similarly, the "Emergency Ballot" slot of the eScan, and its functions, are poorly documented in the user documentation and elsewhere. An "Emergency Ballot" is a ballot cast by voters during a power failure. The eScan has a slot labeled "emergency ballot" to collect and store these ballots. The Hart Use Procedures also direct that Provisional Ballots shall be placed in the Emergency Tray, and directs users to the *Tally Operations Manual* and *Tally Training Manual* (not available for our review) documentation for processing Provisional Ballots.[52] Unfortunately, the *Tally Operations Manual* does not discuss the Emergency Ballot tray at all, and while the Emergency Ballot tray is described—briefly—in the technical specifications documents for the eScan device, most users would not be able to use these documents even if they had access to them. The *Tally Training Manual* was not provided to the Doc Team.

Moreover, the Provisional Ballot use of the Emergency Ballot tray does not appear to be discussed anywhere else in the user documentation other than the *Hart Use Procedures*. While the preprinted post election log forms includes the Emergency Ballot for "un-scanned voted ballots", they do not mention the Provisional Ballot use.[53] And the Provisional Ballot instructions do not mention the Emergency Ballot box. Based solely on the Hart documentation and procedures, Provisional Ballot use—already a confusing part of the procedure for pollworkers—is made even more confusing.

---

[50] *Hart Voting System, System for Election Records and Verification of Operations: Operations Manual, Software V. 4.2*, 6100-102 Rev. 42-62B ("*SERVO Operations Manual*").
[51] *See* the accompanying Hart Red Team and Hart Source Code Review Team analysis in the TTBR.
[52] *Hart Use Procedures*, note 2, Section 8.4 "Canvassing Provisional Ballots", PDF p.38
[53] *See, e.g.*, "Hart Voting System Reconciliation Logs" in *Management & Tasks*, PDF pp.171, 172, 175, 177.

We also note that the documentation specifies that the Emergency Ballot slot should be opened prior to the polls open procedure.[54] This is done so that the security seal on the eScan ballot box door can remain sealed. However, this exposes the box to the possibility of ballots being mistakenly fed into the slot.[55]

4.6 Ability to Assess and Evaluate the System

The documentation provided to the teams included the basic documentation required by the Secretary of State for certification, plus correspondence with the ITAs.[56]

One of the Secretary of State's requirements for certification[57] is that,

> 2. All applications must include full documentation, including technical and operational specifications, operating and maintenance manuals, training materials, and copies of all promotional materials from the vendor."

The documentation must be included on an "Index of System Technical Documentation" that the vendor supplies based on SOS specifications.[58]

However, our evaluation of the documentation indicates that, in fact, this documentation may not be sufficient in all cases to adequately review the system. First, the information is often not equivalent to the TDP submitted to the national certification laboratories. Second, even when the TDP is equivalent to the information submitted to the SOS, it may not be wholly adequate for analyses like the TTBR, which seek to do more than simply ascertain basic functionality of the system.

For the Hart system, proprietary technologies require their own documentation. For example, the RS-485 proprietary connection between the JBC and eSlate terminals requires documentation of the electrical and pinning characteristics of the cabling as well as the communication protocol for the eSlate-JBC data/power path. This document was not available to us.[59] Similarly, the Hart documentation references multiple instances of additional documentation required to fully understand these documents. For instance, each functional or product requirements document for a given component includes references to other documents, most of which we did not have access to.

For this reason, the current level of documentation provided by the California Secretary of State, and requested by the SOS from vendors, does not satisfy the requirements of reviewers that need to be able to independently answer complex technical questions about the system.

---

[54] *Hart Use Procedures*, note 2, p.48 (inspecting the Emergency Tray).
[55] While hardware design is outside of our purview, one quasi-procedural solution to this potential user error might be an external removable covering that could be removed simply (ripped off) without entering the ballot box or relying on electrical power.
[56] With the exception of some documentation that was missing.
[57] *Id.*, note 47.
[58] *Index of System Technical Documentation*, California Secretary of State, November 2006, *available at:* http://www.sos.ca.gov/elections/voting_systems/vsys_cert_applic_part4_1106.doc
[59] A Hart technician was able to provide this information to the Hart Source Team.

4.6.1 Assessment of ITA Reports

At the National level, for many years, the National Association of State Election Directors (NASED) operated a qualification program where independent testing authority (ITA) laboratories would assess voting system compliance with national standards. The responsibilities of the NASED national voting system qualification process were recently assumed by a new federal certification process. The Election Assistance Commission (EAC) oversees laboratories called Voting System Testing Laboratories (VSTLs) each accredited to test by the National Institute of Standards and Technology (NIST) under their National Voluntary Laboratory Accreditation Program (NVLAP). All the systems evaluated in the TTBR were qualified under the NASED process.

In the State of California, all voting systems have to be qualified by a nationally recognized voting system testing laboratory before they can receive state-level certification. In the documents we were provided for the Hart voting systems, we received one software ITA report from CIBER, Inc. (CIBER) covering Hart system 6.2.1[60] and one hardware ITA report, identified as "preliminary",[61] from Wyle Laboratories, Inc. (Wyle) covering system 6.0.

Ideally, a laboratory test report would include enough information to 1) allow a knowledgeable reader to determine that all testing was performed that would be necessary to assess compliance with the standards and 2) permit future evaluators to replicate the testing performed exactly. The ITA reports from the NASED process leave much to be desired in these respects. They do not include extensive information about specific features, controls and measures that a voting system employs to be compliant with specific elements of the VSS. There is very little information about test plans for either state or federal testing activities. The state of the art in this area involves independent approval and publication of a test plan, such as the test plan recently approved and published by the EAC for iBeta's examination of the AVS WinVote voting system.[62] This test plan lists exactly what items they received from the vendor, what tests they plan to conduct, how they plan to document the testing (including an explanatory remark for each NA or NT received)[63] and specific details about specific tests they plan to perform.

4.6.1.1 The Wyle ITA Report

It is disconcerting that the Wyle report is identified as being "preliminary" when a final report should have been issued at some point. We were unable to locate in the documentation provided any final report or system identification number issued by the NASED technical board.

The Wyle hardware qualification test report is for system 6.0, not the system currently under review, system 6.2.1. In lieu of such a report, there is a letter from Wyle that

---

[60] *CIBER Software ITA Report*, note 45.
[61] Wyle Laboratories, Inc., *Preliminary Test Report: Hart InterCivic Hardware Qualification Testing of the Polling Place System 6.0*, 11 January 2006.
[62] *Advanced Voting Solutions WINware Voting System, v.2.0.4 VSTL Certification Test Plan*, iBeta Quality Assurance, as published by the EAC, April 2007, *available at:* http://eac.gov/docs/AVS%20VSTL%20Test%20Plan%2042507.pdf.
[63] *Id*., p.19.

appears to specify that hardware changes made between system 6.0 and 6.2.1 do not require requalification under the 2002 VSS (no system version numbers are mentioned explicitly).[64] This letter includes statements to the effect that Wyle based this determination on documentation from other testing laboratories.[65] However, the specified documentation is not included with the letter, so those who would rely on such a letter have no basis upon which to consider the claim in the Wyle letter credible. In this case, it may be that the small changes made to the eSlate voting booth—adding an aluminum piece so that the eSlate fits better in its cradle and providing a more robust power supply to the VBOx—do not, in fact, require retesting to meet the requirements of the 2002 VSS. However, the full documentation upon which this decision has been made should be available to national and state-level certification authorities.

This letter from Wyle includes a further material inaccuracy. The letter states that the eSlate voting booth was not tested during hardware testing because it was not considered an "active component of the unit." However, researchers have shown recently that the booth is indeed such an active component in that there are wired communication electronics embedded in the booth. Proebstel et al. have shown a number of attacks against the eSlate VBO combination and have outlined possible discrepancies that might occur with the eSlate system as equipped with the VBOx printer subsystem.[66] The eSlate terminal communicates with the VBOx via a connection in the eSlate booth. This communication can be disrupted by physically moving the eSlate terminal so that contact is lost between the eSlate and the VBOx communication path. The Wyle report also contains evidence that the booth/eSlate/VBOx combination was not included in tests to assess the "Common Standards" for accessibility in Section 2.2.7.1 of the VSS.[67]

The Wyle report is also unique compared to other Wyle reports that we have seen. Other reports include some source code review of voting terminal source code. The Hart Wyle report includes no evidence of such a review. On page 12, section 6.3, of the Wyle report, it says that the "precinct-level machine level" firmware was subject to source code review, but by CIBER (the software ITA), and that this review would be included in the CIBER software ITA report. This appears to be a reporting anomaly. The hardware ITA is typically tasked with review of precinct level machinery, including source code. If the hardware ITA does not have the expertise required to perform such a review, it is not improper to contract that portion of the review out to a third party. However, the results

---

[64] Letter from Wyle Laboratories, Inc. (Wyle Letter No. 53097B-009), "Changes to Hart eSlate Voting System Booth", 30 June 2006.

[65] The letter includes statements such as, "Based upon documentation from Percept Technology Labs dated June 28, 2006…" and "… based on documentation from Underwriter's Laboratories Inc. dated June 29, 2006." *Id.*

[66] Elliot Proebstel, Sean Riddle, Francis Hsu, and Justin Cummins, Freddie Oakley, Tom Stanionis, Matt Bishop, *An Analysis of the Hart InterCivic DAU eSlate*, in ACCURATE/USENIX Electronic Voting Technology Workshop 2007, forthcoming, *available at:* http://www.usenix.org/events/evt07/tech/full_papers/proebstel/proebstel.pdf. (Note: the Proebstel et al. analysis covered Hart system 6.1 so these issues may not apply to system 6.2.1.)

[67] On Page A-5-A-6 of the Wyle report, these sections of the VSS are listed as "not applicable". It could be that the eSlate was intended to be untethered and placed in the lap of a wheelchair-bound individual, for example. However, there is a specific type of eSlate/VBOx voting booth with shorter legs that is intended for the DAU (accessible) eSlate that should have been tested.

of such a review should be integrated into the context, form, and results of the hardware ITA report.

The Wyle report includes a lengthy (35 page) appendix that consists of a long list of statements taken from the 2002 VSS and columns of checkmarks for "Accepted", "Rejected", "N/A" (not applicable) and "N/T" (not tested). Unfortunately, when an item is listed as N/A or N/T, there is no explanation given as to why or how the ITA arrived at this decision. In some cases, sections of the VSS are listed explicitly as "Software ITA" and it can be inferred that the Software ITA would test these elements. On balance, these testing designations aren't particularly helpful for one attempting to determine what the testing laboratory tested, how they tested it, and how passing a given test demonstrates meeting the stated VSS requirement.

Some cases involving these designations warrant particular attention. On page A-5 of the Wyle report, section 2.2.5.3 of the VSS, entitled "COTS General Purpose Computer System Requirements", is listed as not applicable. This section of the VSS lists three sets of general requirements for Commercial Off-The-Shelf ("COTS") operating systems. Similarly, on Page A-33, section 6.5.4.1 of the VSS, entitled "Identification of COTS Products", is also listed as not applicable. This section applies to voting systems, like Hart system 6.2.1, that use public telecommunications networks and requires identification of all COTS operating systems, communication routers, modem drivers, and dial-up networking software used in such a voting system. Hart system 6.2.1 uses COTS operating systems and relies on Windows networking software to mediate dial-up communications between the Hart Rally and Tally products. From the documentation, we've been able to determine that the Hart system 6.2.1 uses at least two different general-purpose operating systems (besides Windows itself for the HEMS). The eScan runs on Microsoft Windows CE,[68] an operating system for embedded devices, and the JBC+eSlate combination run on Precise Software Technologies MQX/RTOS for the Coldfire 5307 processor.[69]

It is impossible to tell from the Wyle report what telecommunications functions of Hart's system were tested by the ITA, how they were tested and in what configuration they were tested. In various places in the Wyle report, telecommunications requirements are listed as accepted,[70] not applicable[71] and/or not tested.[72]

From page A-9 of the Wyle report, VSS section item 2.3.1.3.2 (a) "Specifications for ballot materials to ensure that vote selections are read from a single ballot at a time." is

---

[68] In Hart's Product Description document, "PD6000_060_62A.pdf" on page 46 (section 6.5.9), they state that the eScan processor runs "compiled embedded Windows CE code." Also, in both the eScan functional requirements and product requirements documents, they say, the eScan has an embedded processor board "running the Windows CE operating system."

[69] On Page 74 of the CIBER ITA report, it states that the eSlate/JBC version 4.2.13 uses "Precise Software Technologies MQX/RTOS for the Coldfire 5307 processor, Version 2.40"

[70] VSS section 2.5.3.1(g) on page A-14, VSS section 2.5.3.2(d) on page A-15.

[71] VSS section 6.5.2 on page A-33, VSS section 6.5.4.1 on page A-33 and all of VSS section 6.6 on pages A-35-A-37.

[72] VSS section 2.2.10 on page A-8, VSS sections 5.2.1-5.2.7 on pages A-30-A-31 and VSS section 6.5.4.3 on A-33.

marked as not applicable. In the CA State's Consultant's report,[73] an issue is listed where the eScan optical scan system will accept two ballots in succession after a ballot has been rejected and the pollworker pushes the override button to accept the ballot with errors. This can result in the second ballot not being scanned at all because the eScan keeps the digital image of the error ballot in memory until the error condition is cleared or the ballot is submitted with an override. This item is under VSS section 2.3.1, which is considered by the ITAs to be entirely the purview of the Software ITA. However, this is a good example of an incident 1) where the division of labor between hardware and software ITA resulted in serious problems slipping through the cracks of the national certification testing process, and, 2) that demonstrates the importance of systems-level functional testing by individuals with extensive election experience using the equipment in a real-world scenarios.

Section 3.2.2.15 of the VSS, entitled "Data Network Requirements" is listed as not applicable despite the JBC using a local network to communicate with eSlate terminals, Ballot Now being configurable in a client-server architecture for scanning of absentee ballots and Rally clients communicating with a Tally machine for communication of MBB summary results over a local or remote, dial-up network. Similarly on page A-33, VSS section 6.5.2, entitled "Data Integrity" covering transmission integrity checking of vote data, is listed as not applicable.

Feldman et al. demonstrated the first viral attack against a voting system using PCMCIA memory cards.[74] On page A-33 of the Wyle report, VSS section 6.4.2, entitled "Protection Against Malicious Software", is listed as not tested.[75] This section of the VSS requires voting systems to employ protective measures against "file and macro viruses, worms, Trojan horses, and logic bombs". The lack of ITA testing could very well be a result of such a requirement not being easily testable. However, some basic protection, verification and authentication would drastically reduce and inhibit many types of malicious software, and there's no evidence that Wyle conducted any testing with respect to protective measures.

Appendix B of the Wyle report covers Percept Technology Labs' (Percept) testing of the VBO (although they really appear to have testing only the VBOx printer and not the entire VBO booth). On page B-15, the report states:

> **Note A: During the Lightning Surge Tests, the printer can be made to print out a "ballot accepted" heading with an associated bar code or human readable ballot information when a surge occurs. In the case when the 'ballot accepted' bar code is printed, the tabulating software detects the presence of a duplicate bar code and only accepts one of the registered votes. If the surge causes a human readable

[73] *See* page 5 of: Paul W. Craft and Kathleen A. McGregor, "California State Consultant's Report on Hart InterCivic System 6.2", August 4, 2006; Paul W. Craft, "California State Consultant's Report on Hart InterCivic System 6.2.1", September 5, 2006, *available at:* http://www.sos.ca.gov/elections/voting_systems/hart_621_consultants_report_final.pdf.

[74] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine*, in USENIX/ACCURATE Electronic Voting Technology Workshop 2007 (EVT'07), *available at:* http://www.usenix.org/events/evt07/tech/full_papers/feldman/feldman.pdf.

[75] This section is listed as the responsibility of both the "(Hardware and Software ITA)" in the Wyle report.

ballot to be printed, it will be followed by a ballot rejected printed notice and bar code. This satisfies the requirements of the VSS requiring no loss of voter data."

It is unclear if Wyle (or Percept) in this case is using the VBOx configured to include serial numbers in the barcode.[76] Accordingly, it is unclear whether or not the tabulating software would detect duplicate bar codes if the system were configured without a serial numbers encoded in the barcode. This statement also seems to draw a connection between the presence of barcodes and their significance in tabulation; we were able to find no such facility in the eSlate system that tabulates election results based on reading barcodes.[77] Finally, researchers have since discovered that jostling the VBO booth in such a manner that disrupts the communication path between the eSlate terminal and the VBOx printer produces similar results.[78]

4.6.1.2 The CIBER ITA Report

CIBER's software ITA report for Hart system 6.2.1 includes functional testing and source code examination of all software elements of the Hart system except COTS products. As we noted in the Wyle section, the precinct level software[79] review required of the hardware ITA is included in this report instead of the Wyle report.

Page 3 of the CIBER report states, "CIBER has an interim accreditation as an ITA through the National Association of State Election Directors (NASED)." This is likely incorrect. The EAC accredited existing NASED ITA laboratories on an interim basis during the transition period between the NASED-overseen and the EAC-overseen processes. CIBER never achieved accreditation under either the EAC's interim process or the EAC VSTL process.[80] Unfortunately, there is not enough public information about the internal workings of the NASED process[81] to say if NASED had an interim accreditation program.

A list of software and hardware for system 6.2 is listed on page 5 of the CIBER report, including the COTS operating systems for the HEMS software and the scanners and

---

[76] Hart calls their ballot-specific serial number a "Ballot Key". California requires the Ballot Key to be disabled during election definition so that individual VVPATs contain no individually identifying information. See the *Hart Use Procedures*, note 2.

[77] There are comments on possible future products in this vein in Hart's functional and product requirements documents for the VBO.

[78] *See* Proebstel et al., note 66.

[79] This is often called "firmware" in the NASED ITA process.

[80] The first two laboratories, SysTest and Wyle, were not issued interim accreditation until 8/15/2006 (*See:* "U.S. Election Assistance Commission Interim Accredited Voting System Testing Laboratories", August 28, 2006, *available at:* http://eac.gov/docs/Interim%20Accredited%20Test%20Lab%20info%20for%20Web%208-28-06%20-%203.pdf). CIBER was notified that it was deficient via a NVLAP report on July 20, 2006. (*See:* "Election Assistance Commission Interim Accreditation of Independent Test Authorities Assessment Report for CIBER and Wyle", July 22, 2006, *available at:* http://eac.gov/docs/Ciber%20&%20Wyle%20Assessment%20(July%202006).pdf) and was formally notified by the EAC of deficiencies on September 15, 2006 (*See:* "EAC Letter to CIBER", September 15, 2006, *available at:* http://eac.gov/docs/EAC%20Letter%20to%20Ciber%20(Sept%202006).pdf). CIBER's application for interim accreditation was terminated on June 13, 2007 (*See:* "Commission Votes to Terminate CIBER Interim Accreditation", June 13, 2007, *available at:* http://eac.gov/docs/6-13-07%20-%20Commission%20Votes%20to%20Terminate%20CIBER%20Interim%20Accreditation.pdf).

[81] NASED is a private organization and conducted their work largely on a volunteer basis.

printer used for Ballot Now. However, none of the other COTS operating systems identified above are listed, notably Windows CE for the eScan and MQX for the JBC/eSlate. Only unmodified COTS software is exempt from certification review[82] and there is no evidence that CIBER made any findings about the status of COTS software.

There is tentative evidence that Hart's MQX may not be COTS. In order for components of a voting system to meet the VSS definition of COTS,[83] it must be "readily-available". Hart apparently owns and controls the source code for their version of MQX but we could not find evidence that Hart has made it readily available.[84] It appears that CIBER was not provided with the source code for MQX; neither was the TTBR Hart Red Team.[85] If Hart has made modifications to its version of MQX, it should be subject to source code review.

On page 8 of CIBER's report it states, "The application does not allow reuse of cards or incorrect sequencing of cards." This does not seem quite right; in our walkthrough exercises[86] we reused cards all the time by writing over their contents with BOSS. This would make sense if they meant that cards could not be reused within a given election.

The summary of functional testing on page 11 of CIBER's report is not adequate. The comments at the beginning of this section about what level of description is needed to replicate functionality testing apply here. Even what is included is inadequate. For example, CIBER only seems to do one kind of regression test which tests end-to-end functionality; regression testing typically also includes a test suite which is designed to expose previously corrected bugs, errors and dependencies.

It appears that CIBER did do some substantial document review and found some issues when comparing functional requirements and operating manuals. Evidence of this review is on page 12:

> The documents included in the TDP review are listed in Section 3 of this document. Only minor anomalies were found (discrepancies between component functional/requirements specifications and associated operations manual) and these were noted and sent to Hart. The anomalies were addressed by Hart and resolved.

However, from the information given, it is impossible to tell what those deficiencies were and if they were resolved appropriately.

It is clear that CIBER's source code review is not intended to examine much more than software quality, and then only in form, not function. On page 13 of the report, CIBER

---

[82] VSS, note 1, section 4.1.1.

[83] The VSS (note 1, p.A-3) defines COTS as, "Commercial, readily-available hardware devices (such as card readers, printers, or personal computers) or software products (such as operating systems, programming language compilers, or database management systems)."

[84] "The source code for [the MQX] operating system is currently owned and maintained by Hart InterCivic." *See Hart InterCivic Direct Recording Electronic (DRE) & Voter Verifiable Paper Audit Trail (VVPAT) Technical Security Assessment Report*, Compuware Corporation for the Ohio Secretary of State, December 2005, p.12, *available at:* http://www.sos.state.oh.us/sos/hava/hart121305.pdf.

[85] The CIBER report (note 45) only lists two, presumably trivial, files that appear to be related to MQX: "mqx.h" in Hartlib and eScan; "MQX_INIT.cpp" eSlate/JBC.

[86] *See* section 5.1, *infra*.

states, "The source code review is an evaluation for compliance with FEC guidelines and Hart InterCivic standards for software quality." However, the list of elements that they design their review to examine include mostly issues of software quality such as "Selection of programming languages", "Software integrity", "Software modularity and programming", "Control constructs", "Naming conventions", "Coding conventions" and "Comment conventions". Nowhere listed are items related to software security and reliability such as "Buffer overflows".

On page 13, CIBER notes that Hart uses the C++ and PowerBuilder programming languages. PowerBuilder "p-code libraries" are used in BOSS[87] and are considered interpreted code; they are interpreted by the PowerBuilder Virtual Machine. While the VSS prohibits "self-modifying, dynamically-loaded, or interpreted code"[88] there is an unclear exception to this rule in the VSS (pointing to a non-existent section "6.4.e") that leaves the status of PowerBuilder interpreted code in the air. Interpreted code poses a particularly high risk when used on removable media that might change hands in environments of questionable security.[89] Fortunately, the PowerBuilder code is never placed on removable media and the BOSS server enjoys a particularly tight security environment. We would expect a security review to have identified the presence of this code and assessed its security implications.

In CIBER's description of their functional test approach in Appendix C (page 17) they say, "… test cases exercised all of the *added functionality* of the Hart InterCivic system …". However, in order to capture regression of past issues, all the past tests should be rerun to evaluate regression in other areas, not just features added. Also, in the same section, CIBER says that they used election definitions from "previous system integration testing efforts" instead of creating them using the new versions of BOSS, the Hart software that is used to define elections.

4.6.1.3 Is the ITA documentation adequate?

In general, we have identified a number of major problems with the ITA reports for Hart system 6.2.1. We cannot assess from the documentation provided if the review was adequate. Further, there is evidence that specific issues were missed and either identified during state-level certification or, in the case of the findings of the accompanying TTBR team reports, never at all.

First, they do not contain enough information for a reader to determine if the tests they performed were adequate in terms of assessing compliance with the 2002 VSS. Only in the case of CIBER is any test case or test plan presented, and then what is presented is not at the level of detail one would need to replicate their tests. There is no data or performance output for functional testing in the CIBER report. The Wyle report describes the functional testing performed in terms of checkboxes for accepted, rejected, not applicable and not tested. As a threshold issue, the checkboxes are not useful without

[87] P-code library files have "pdb" extensions; see page 24 of the CIBER report.
[88] VSS, note 1, Section 4.2.2.
[89] David Wagner, David Jefferson, Matt Bishop, Chris Karlof and Naveen Sastry, *Security Analysis of the Diebold AccuBasic Interpreter*, California Secretary of State Voting System Technology Assessment Advisory Board (VSTAAB), February 14, 2006, *available at:* http://www.sos.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf.

descriptions of the testing performed and results achieved that would demonstrate compliance for a given requirement.

Second, the information they do contain is not particularly useful. Our companion source code review team and red team asked us in a few cases about the configuration of the Hart system during the ITA testing. In all but the most basic cases, we were unable to determine configuration parameters. For example, whether they had serial numbers configured in barcodes or not, which is a California-specific configuration requirement. Test plans and reports should indicate at a very fine level of detail the exact configuration of the voting system for the tests they conducted. In addition, the CIBER source code review states the system passes source code review with little to no evidence of how they performed their review, what kinds of resources it entailed, and the detailed outcome and implications of their findings. Quality source code review includes line numbers of specific security, reliability and quality violations for specific files and includes commentary on detailed review methodologies and tools employed in the review process.

Third, certain problems make it through the national process untested that should have been identified and tested. The ballot handling issue[90] and the lack of testing of certain telecommunications requirements[91] and malicious software requirements[92] are each evidence of these holes in the process.

Finally, it appears that the division of labor between two or more evaluation laboratories might reduce the overall quality and comprehensiveness of the assessment. Items on the Wyle checklist are often clearly marked for either the software or hardware ITA only, despite some of these requiring more than just source code review or more than hardware environmental or functional testing. It seems that contracting out small, specialized evaluation activities, such as the electrical testing of the VBOx by Percept, poses less of an opportunity for complex division of labor problems.

4.6.2 Assessment of State Reports

California has in the past hired consultants to evaluate voting systems as to whether they meet requirements specific to California elections and, increasingly, to catch problems that might have escaped the inadequate testing performed at the national level. The consultants produce a report[93] (Consultant's report) after testing the system at issue and then the Secretary of State's staff interprets this report and other information to produce a report[94] (Staff report) that recommends certification (or non-certification), sometimes conditionally. The Secretary of State then issues a certificate that allows a voting system to be used, subject to conditions, in California elections.[95]

---

[90] *See* discussion surrounding note 73.
[91] *See* discussion surrounding notes 70-72.
[92] *See* discussion surrounding notes 74-75.
[93] *See* Consultant's Reports, note 73.
[94] *Id.*, note 73.
[95] *See Hart Certificate*, note 10. Note that the certification for Hart system 6.2.1 specifically excludes Hart's Bravo, Fusion, In-Fusion and Trans software. In a number of places, the documentation, especially the operator's manuals, includes references to these products. This seems reasonable considering it might be onerous to require a state-specific set of operating manuals. However, jurisdictions should always look to the Hart Use Procedures for their system in conjunction with these operating manuals.

4.6.2.1 Consultant's Report

The consultant's testing and subsequent report appears to have been critical in terms of identifying issues either specific to California elections or problems that made it through the national process. We were impressed with the subtlety of some of the issues they identified, many of which we also discovered or experienced during our walkthrough exercises[96] with the Hart system.

The general criticism involving lack of information necessary for test reproducibility of the report applies here as well as to the ITAs.[97] For example, page 2 of the consultant's report says, "The results described in this report should be reliable and repeatable for [the] specific items [of system 6.2.1]." However, there is not enough data about the details of the tests performed to repeat these tests. The consultant's test plans are attached to the *staff report*, curiously, and include only general descriptive titles about actions to be performed with the system, not detailed configuration descriptions, setup data and output. That aside, we describe one other issue we identified.

On page 5 of the report, it says, "There were eight printer error anomalies. […] The cryptic error messages noted in the testing of version 6.1 of the system still exist." Error messages are regulated by VSS section 2.2.5.2.2 (b)-(e), which say, in part:

> All error messages requiring intervention by an operator or precinct official shall be displayed or printed unambiguously in easily understood language text, or by means of other suitable visual indicators; […] The message cue for all systems shall clearly state the action to be performed in the event that voter or operator response is required;

In addition to this issue, there are a number of comments in the consultant's report and the incident log for volume testing where the consultants recommend that a particular issue should be addressed by the *Hart Use Procedures*. On balance, these items did not make it into the Hart Use procedures. Instead of itemizing those issues here, we have placed them in other sections of the document.[98] Before use procedures are formally accepted as final, the Secretary of State's staff should ensure that all items in the consultant's report and in state testing incident logs are addressed so that election officials do not run into these issues without warning and adequate preparation.

4.6.2.2 Staff Report

The Staff report essentially repeats the findings of the consultant's report, but embeds those findings and other information in the legal and regulatory context of California in order to make a recommendation to the Secretary of State as to certification and any conditions that might be imposed upon the system as certified.

The only comments we have about the Staff report are process-related rather than substantive. First, when comparing the Hart Staff report with the two staff reports for the Diebold Election Systems, Inc. (DESI) and Sequoia Voting System, Inc. (Sequoia) there

---

[96] *See* section 5.1, *infra*.
[97] *See* section 4.6.1, *supra*.
[98] *See* notes 124, 172 and 182 and surrounding discussions for examples of where items listed in the Consultant's Report or volume testing incident logs failed to make it into the use procedures.

were significant differences. Notably, in the other two reports there were references to a document, apparently used in the past by the California Secretary of State, entitled, "Procedures for Approving, Certifying, Reviewing, Modifying, and Decertifying Voting Systems, Vote Tabulating Systems, Election Observer Panel Plans, and Auxiliary Equipment, Materials, and Procedures".[99] This document seems to have been used by Secretary of State staff in assessing whether or not a voting system met all the requirements specific to California legislation and regulation and the Secretary of State's own policy. We were unable to determine why this document ceased to be used by the Secretary of State's staff in certification, nor the genesis of the elements in the document.[100]

Second, page 9 of the Staff report states, "The test plans for those examinations are included as an appendix to this document." However, as noted above, the test plans are more like outlines of testing actions than detailed testing plans. They consist of an outline of a set of actions to be performed in order. The documentation, data and other information surrounding these actions would be necessary to replicate the testing performed in detail.

4.6.2.3 Is the State testing documentation adequate?

In general, we have few criticisms of the quality and comprehensiveness of the state testing documentation. Naturally, the scope of state testing is narrower compared to testing conducted at the national level. When the state testing consultants find issues with a submitted voting system they are very clear about the conditions under which the issue occurs, technical measures needed to avoid it and what action should be taken at the policy level. When an issue necessitates a technical change, they are clear about what the issue was, what fix was implemented and the circumstances and outcome surrounding any need to re-test. The only area in which we find these documents lacking is in the documentation of the test plan and data needed to reproduce their tests. For example, in the Hart system one issue noted by the consultants was that a voter using an audio ballot and casting a write in could have a different letter of the alphabet read back to them than what they selected if the focus changes quickly after selection (that is, if the voter turns the selection wheel slightly after pressing the enter button). There is no evidence of specific test actions designed to identify loss-of-focus issues and discrepancies in the consultant's test plan. A list of such test actions would be very useful for other states that would like to perform comprehensive functional testing of voting systems.

---

[99] This document is no longer available on the Secretary's web site. The authors have made it available here: http://josephhall.org/vsp_procedures-20060502.pdf. This document was last available on the Secretary's web site in May 2006 and first appeared in September 2002 (the document appears not to have changed over this time period; each has the same md5sum hash: 80438f52db342e896759b4f171175862). Lowell Finley, the current Deputy Secretary of State for Voting Systems Technology and Policy, was able to point us to copies of this document using the Internet Archive's Wayback Machine. *See*: http://web.archive.org/web/*/http://www.ss.ca.gov/elections/vsp_procedures.pdf.

[100] Some are clearly from the California Election Code, the California Constitution and Federal election laws.

5 Sufficiency of Documentation

We reviewed the system documentation, including user operation manuals, support manuals, technical specifications, and supporting materials, to see if the documentation, as a whole, generally supported election officials and pollworkers in ensuring the successful completion of election tasks ("Usability"); the accuracy and reliability of election equipment and results ("Accuracy and Reliability"); the security of the election ("Security"); the secrecy of individual voter information ("Secrecy"); and the auditability and verifiability of election events ("Auditability"). In general, this involved consideration of whether the documentation contained information and procedures to conduct normal operations and to troubleshoot exceptional operations; and whether procedures existed to prevent, mitigate, detect, or respond to vulnerabilities.

5.1 Usability

A system's documentation is usable if it documents the system such that a system's user is able to complete specific system tasks efficiently, effectively, safely, and satisfactorily. The team reviewed the documentation carefully in a phase-based analysis where each phase of the election process has different requirements. We then used the system documentation to conduct two walkthroughs of an election using the system 6.2.1 equipment and software, from ballot definition through tabulation of election results.

Usability of documentation depends principally on the print documentation, but also relates to the user interface, error messages, help functionality, default configurations, and feasibility of the suggested operations and procedures. For instance, if the user interface is complex and not self-explanatory, then the documentation is only usable if it clearly explains how to navigate the user interface. Similarly, if the user interface is markedly different than described, then documentation is less usable. If the print documentation is based on an assumed state of configuration, but the default or system-specific configurations are different, then the user may be confused because the documentation is less usable with the system as configured. If error messages show up on screen that are not documented then, again, the user may be confused. If the suggested procedures miss important steps or are not adequately described, then the user may be confused. These are all examples of heuristics that can be used to assess document usability.

5.1.1 General Comments on Hart Documentation Usability

5.1.1.1 Online Documentation

In the TTBR evaluation configuration of equipment,[101] online context-specific help was largely nonexistent. While the "Help" menu item was present in many of the HEMS software products, many provided no information or behaved as if they required internet access to function. Naturally, the computers running the HEMS must not be connected to the internet, in order to avoid exposure to malicious software.

Help functionality is a useful documentation feature since it provides users with a way of instantly accessing information from within the problem screen. Help can be made

[101] As reviewed in Sacramento, June 3, 2007.

context-sensitive, which aids the user by taking them directly to the help for the active module or step. In the absence of online context-sensitive help, printed documentation is particularly critical.

We recommend that help functionality be installed locally so that an Internet connection is not required and that this functionality be tested in both state certification and acceptance testing.

5.1.1.2 Printed Documentation

Hart's printed documentation is generally clear, accessible, and well written.

However, general system-wide information location aids are lacking making it difficult to find information about particular topics, features, or software that crosses over multiple EMS applications. Indexes and glossaries within individual documents are helpful but do not substitute for the ability to locate an item anywhere in the documentation set—a feature particularly important for election officials managing the system overall. The user documentation is distributed over fifteen documents which we were provided: six software manuals; one product description; four software training manuals (not provided); two pollworker desk references; one *Support Procedures*; one *Management & Tasks* procedures manual; and the *Hart Use Procedures*. Several of these documents are in the 300-600 page range. Locating the right procedure or information in a timely manner can be difficult without some comprehensive index.

Similarly, no one single glossary was available to users. Instead, partial glossaries were distributed across multiple sources of documentation, and in inconsistent locations. For instance, the software manuals (e.g., *Tally Operations Manual*, *Rally Operations Manual*, *Ballot Now Operations Manual*) each included an "Important Terms To Know" section, but Tally's was listed as Table 13, page 32, and Rally's was Table 1, page 21. The *Management & Tasks* document included a "Glossary" as Appendix A. The "Glossary of Terms" in the *Support Procedures*[102] was the largest and most comprehensive, but still missed material included in other glossaries. The context-sensitivity of the individual glossaries was helpful, but leaves the problemof the lack of comprehensive materials to accompany the software-specific materials.

In general, the documentation would likely be improved by surveys of or input from users on the ground.

5.1.1.3 Procedures

Hart logistical instructions and procedures for basic operations are generally clear and thorough. The documentation is generally well written and precise. It includes sample workflows, floorplans, and connection diagrams for most needs. It includes numerous sample forms and logs to be used in conjunction with its procedures, helping to maintain security and auditability (see below in relevant sections for additional discussion).

However, while the instructions for basic use are generally good, troubleshooting sections and information about exceptional situations was much less useful. In our walkthrough roles as "election officials" (defining ballots and tallying votes);

[102] *System Support Procedures*, note 22, "Glossary of Terms", pp.251-262 (PDF pp.257-268).

"pollworkers" (opening and closing the polls; issuing access tickets; recognizing and dealing with problems at the eSlate and eScan); and "voters" (casting ballots), the documentation did not anticipate many problems we experienced.

Procedures for maintaining accuracy, security, secrecy, and verifiability are not always clear. For instance, forms may include some information; checklists other information; the *Hart Use Procedures* still yet other critical information. When the basic essential steps to run an election are dispersed through multiple documents and styles of documentation, it is difficult to ensure that all of them are followed.

Moreover, many procedures—such as recounts or audits—are poorly documented in the materials we were given to review. Some of these materials may be included within the Training Manuals, which we were not given. We were thus unable to evaluate or assess many procedures.

The procedural documentation includes very little information in the text about context, rationale, or consequences. For instance, it is rare to see user warnings or alerts about procedures that could implicate accuracy, reliability, security, secrecy, or auditability.

In the following sections, we comment in detail about our findings relating to specific election procedures and phases. (See Figure 1, supra Section 3, for overview of the election phases.)

5.1.2 Certification Procedures and Documentation

Certification requires disclosure of COTS software used. Documentation in the system states throughout that it uses a "commercial third-party database" in BOSS and other HEMS systems (for example, the Voting System Product Description, PDF p.9). Our walkthrough activities determined that this was a Sybase database. The documentation does not specify the specific COTS product, contrary to the VSS requirement to specify all COTS by name and version number.[103]

In general, because documentation includes the procedures for operation, it can significantly affect the performance of the system—not just its usability, but its reliability, security, privacy, and auditability. That is to say that election officials need to have documentation that has been vetted just as thoroughly as software and hardware. Therefore, we recommend that recertification or re-approval of some sort should be considered for changes to policy or procedures in documentation that define sensitive or otherwise critical operations.

5.1.3 Installation and Upgrade Procedures and Documentation

Hart installs and configures the hardware and software.[104] Hart is also responsible for virtually all hardware, firmware, and software upgrades, with two kinds of exceptions which are done by local officials: (1) virus definition upgrades, and (2) products which can be installed on multiple machines, such as Rally.

The user documentation generally provides very little information about Hart's hardware and software installation procedures. In particular it's unclear whether the counties buy

[103] *See* discussion surrounding note 68.
[104] Customers may install additional copies of Rally on workstations as needed.

their own Windows machines and Hart comes in and installs HEMS, or whether the county signs a contract with Hart and Hart provides the machines as part of the procurement agreement.[105] This can significantly affect the issues relating to configuration and installation of Windows. For instance, the *Hart Use Procedures* require disabling a number of Windows networking and communication protocols. But this is not documented elsewhere in any of the Hart user and training manuals. Unless Hart staff does this configuration, it may easily get missed by elections officials who are carefully following the *System Support Procedures* and *Management & Tasks*.

The software applications can apparently be installed in numerous configurations. For instance, the *Hart Voting System Support Procedures Training Manual* ("System Support Procedures") discusses individual computers running BOSS, Rally, Tally, and SERVO.[106] The configuration that the TTBR team used included a laptop running BOSS, Ballot Now, Tally, and eCM Manager; and a second laptop running Rally and SERVO.

5.1.4 Initial Security Procedures: Passwords and eCMs

A factory signing key is programmed to the voting devices for shipment.[107] When the systems are first received by a jurisdiction, the jurisdiction must reset passwords using statutory specifications.[108] Each of the secrets normally kept for an election—passwords, PINs, encryption keys, modem numbers, etc. —should be changed before subsequent elections to help ensure that learning one of these secrets only has implications for one election. When first setting up an election, a new eCM key should be generated.[109] This should be done in advance of election setup.

5.1.5 Training Documentation and Procedures

The training manuals for the Hart EMS software products were not provided to the TTBR Documentation Team, and could not be evaluated. The *Management & Tasks* and *System Support Procedures* documents included some information about training programs (available for purchase) and training documents.

5.1.6 Election Setup Procedures and Documentation

The user documentation for setting up and defining an election using BOSS appears adequate for a basic no-frills election. The *BOSS Operations Manual*, along with the *Management & Tasks* reference, include enough information to define a simple election database, generate the electronic ballots, write the MBBs, and finalize the database for reading by Tally.

---

[105] Specific configurations of California counties were out of scope for our review. However, we note that Hart's online contract with Texas includes sale prices for computers to be used with the Hart EMS. *See* Hart InterCivic online Texas catalogue note 15.
[106] *System Support Procedures*, note 22, pp.27-28 (PDF pp.33-34).
[107] *Id.*, p.44.
[108] *Hart Use Procedures*, note 2, Section 3.3.1 (p.14).
[109] There does not appear to be any technical restriction that forces the user to generate a new eCM key for each election. However, the *Hart Use Procedures*, note 2 p.17, advise that "A new signing key must be used for each election."

As in other Hart documentation, the *BOSS Operations Manual* is generally well-written and, we believe, understandable by the intended audience (election officials and staff).

The *BOSS Operations Manual* is greater than 500 pages long, which is comprehensive but unwieldy. However, the documentation does include a comprehensive index. Spot-checking the index found most items needed, under logical headings. As with other HART documentation, the *BOSS Operations Manual* would benefit from additional summary information and short topical indexes. For instance, "Sequential Steps for Creating an Election in BOSS" is quite helpful,[110] but is the only step overview in the manual. In the *Ballot Now Operations Manual*, by comparison, the "Sequential Steps for Tasks" includes short tabular form task lists for each of the half-dozen or so tasks.[111] Similar step-by-step overviews for subprocesses and relationship to other programs would improve the usability of the *BOSS Operations Manual*, which is both at the heart of and one of the more complex components of the Hart EMS.

In the absence of short overviews and contextualizing information, our walkthrough tests were not as easy as they should have been, and setting up a more complex system proved difficult in our walkthroughs. User interface cues were also sometimes not available, causing momentary confusion.

Software defaults were sometimes not set in the obvious or correct setting, raising the possibility of unnecessary error. (This may be an artifact of our study environment, because we had no access to information about county-specific installations.)

In BOSS, for example:

- The *Hart Use Procedures* and system documentation describe how set eScans to provide warning of over- or undervotes but the default is set to ignore warnings.[112] Overvote notification should enabled by default on eScans to minimize disenfranchisement of communities that tend to cast overvoted ballots.[113] Other software configuration issues include the "VBO required" option, which was left to the user even though it is not optional in California, and the system choice of a state, which is not variable in California.
- The system generally employs a 24-hour clock, which is useful for precise and clear definitions of time. However, for users who are not expecting a 24-hour clock, an AM/PM indicator and 12-hour clock in parentheses ensures there is no confusion. This is important, for instance, in defining election open and close times. An election official user programming the MBBs who wishes to open an election at 6am, and close it at 8pm may choose "6" and "8" without considering that "8" is 8 *a.m.*, and that "20" is the proper closing time.

[110] *BOSS Operations Manual*, note 13, Table 1, p.39.
[111] *Ballot Now Operations Manual*, note 17, pp.28-30.
[112] *Hart Use Procedures*, note 2, p.15; *BOSS Operations Manual*, note 13, p.131.
[113] Lawrence Norden, Jeremy M. Creelan, David Kimball and Whitney Quesenbery, *The Machinery of Democracy: Usability of Voting Systems*, Brennan Center for Justice at NYU School of Law, 2006, p.U-4, *available at:* http://www.brennancenter.org/stack_detail.asp?key=97&subkey=36941.

- When setting up an election database in BOSS, the registered voter total per party doesn't update the count until you click again in the window.[114]
- BOSS provides no warning or indication about the status of MBB cards and whether they have election definitions on them already, or not. Thus, it is possible for a user to write and rewrite elections on the same card, by accident.
- When generating ballots in BOSS, the review process before finalizing ballots is confusing. It permits you to review them, by paging through the ballots; but the "ACCEPT BALLOT" button accepts *all* the ballot definitions for that election, whether or not the election official user has paged through or reviewed all the ballots. When there are multiple ballot definitions for different styles / precincts, this can be quite confusing, since the placement of the button suggests that "ACCEPT BALLOT" will accept just the current ballots. No warnings clarify that this button accepts and finalizes all ballots.

While any one of these user interface issues may be a relatively minor problem, they are exacerbated in the Hart system by the "Finalization" procedures. When a database has been fully defined, it is "Finalized", which prevents further changes to the database. This is an important security precaution, but it means that the user *must* have defined things correctly—or they have to go back and redo the system from scratch. For this reason, Hart recommends making "backup" copies of un-Finalized databases;[115] these "backup" the database in an editable mode. This ameliorates the problem—though it raises security implications, which are discussed below—but user interface cues, warnings, and correct default settings would be greatly preferred to reopening a "rough draft" database which may, itself, have been subject to additional alterations or tampering.

5.1.7 Printing Ballots

After proofs are approved and ballot definitions are finalized in BOSS, the election official uses one of the BOSS-generated MBBs to open up an election database in Ballot Now. This election database will be used to reconcile ballots, to print ballot proofs to send for printing, and to print on-demand ballots.

The user documentation for Ballot Now again was based on a problem-free installation, and appears adequate for basic use of the system. However, our walkthrough with Ballot Now was not problem-free, and stressing the system with reasonable user errors (both intentional and unintentional) very quickly led to confusion and difficulty.

For instance, when loading an election in the system, without clearing out the previous election, we got an error message indicating that Ballot Now saw a preexisting election ID. The message instructed the user to eject the MBB media, restart Ballot Now, and delete the preexisting election. (Error message: "election database nonexisting or deleted".) After deleting what we thought was the preexisting election, ejecting and restarting, Ballot Now still wouldn't start and requested that we "manually delete the election files". We were unable to find user documentation to assist with this process, and ended up going through the DOS prompt and Windows file manager to browse

[114] This was our experience during the walkthrough activity.
[115] *Management & Tasks*, Chapter 3: Software Administration Tasks, "BOSS Database Management" (pp. 51-53).

directories and choose which files to delete in order to get the system to work. Even at that point, we were still unable to open the system. We then opened up audit logs in BOSS to find likely directories, and deleted those files. After a few more rounds of error messages, Ballot Now crashed and wouldn't open further with that election. We had to redefine the election, created a new database and burn new MBBs.

These problems could have been resolved with clearer documentation regarding the unique identifiers for elections. For instance, each election is assigned an "Election ID." However, it is unclear from the documentation when the two-digit "Election ID" is assigned by BOSS, how a user would determine the Election ID of a recently created database and how that number is generated. It appears to be semi-sequential, since the elections we created were consecutively numbered 51, 54, and 52; however, it is either not fully sequential or the sequentiality can be defeated by user error.

5.1.8 Database Backup Procedures and Documentation

Hart includes numerous admonitions to make backups of data and databases throughout its documentation. Hart includes integrated "backup" and archive functionality in several of its EMS programs—BOSS, Rally, and Tally—but not all. Ballot Now, eCM Manager, and SERVO do not have integrated functions to backup their databases. (SERVO's extensive back-up capability is backing up equipment, not its own databases, which include equipment inventory and its backups of equipment memory.)

Backups are suggested both for redundancy security and to facilitate starting over from scratch. In a complex system such as BOSS' election definition process, certain mistakes might require the whole procedure to be started again. For instance, if VBO required was not checked before the election definition was "finalized", then the election would have to be completely redone.

Hart recommend making a copy of the system just prior to finalizing, to minimize the problem of having to recreate a database from scratch if errors were made. While this procedure does remedy the problem of having to completely start from scratch in defining an election, it also creates a duplicate, unfinalized election system. This may cause some security risks, which are discussed further in the Security section.

5.1.9 System Configuration

Different system configurations could expose applications to different risks. For instance, Rally and Tally are supposed to run on equipment with a modem port. SERVO, however, does not require a modem. Similarly, SERVO requires an ethernet port. In theory, it seems possible that virtually all the software could run on one machine. Recommended configurations, or cautions about configuration, were not discussed, presumably because Hart controls the basic installations. However, documenting software incompatibilities or recommendations could help elections officials, who may be tempted in some circumstances to install additional copies of the applications on various machines.

Similarly, the hardware options are not well-documented. For instance, the SERVO manual (and the System 6 preliminary documentation) both reference different types of JBCs. The JBC 1000B has a modem; the JBC 1000 does not have a modem.[116]

5.1.10 Error Messages

Error messages were not always helpful. For example, when burning media, bad media generates the message "bad card detected—the window does not have scrollbars." "Bad card detected" is clear enough, but the additional comment that "the window does not have scrollbars" can be confusing, suggesting to the user that there is some potential software fix for the problem. In this instance, bad media is not fixable by the software, and a fix *should not be* attempted: malfunctioning election media should be removed from the election process.

5.1.11 Configuring Polling Place Hardware

SERVO uses the election-specific MBBs to configure JBCs and eSlates.[117]

eSlates are wiped clean by SERVO, their public count is reset, and the Key GUID is copied to them, but they do not generally receive any other configuration information. Instead, eSlates are generally run by software on the JBC. ESlates may be run in "SOLO" mode, in which case an MBB is inserted into the eScan itself.

During configuration, batteries are installed in JBCs, eSlates, DAU eSlates, and eSlate VBOs. Printer paper is installed in JBCs, eScans, and the eSlate VBOs. The eScan scanner path must be cleaned with pressurized air, and the Ballot Now scanner path must be cleaned "according to the scanner manufacturer's procedures."[118]

MBBs may be left in the polling place hardware and delivered with MBBs intact, or polling place hardware may be delivered with MBBs installed later.

SERVO's resetting process is optimized for rapid processing of equipment. This is useful for the set-up of equipment, but dangerous when SERVO is being used to back-up CVRs and audit logs from equipment.[119]

In at least one instance, a critical basic maintenance step—cleaning the scanners—is insufficiently highlighted. Both the Ballot Now and the eScan documentation include the step to clean the scanners. This is important—if it is not cleaned, then sections of ballots can be obscured or misread. However, without some contextualizing information or an alert that highlights the critical nature of this step, it may be overlooked or minimized. In the worst case, it might be skipped by a hurried election official worried simply about making sure the machines *work* on a mechanical level—without fully understanding the ways that seemingly minor technical maintenance can have unanticipated effects.

Hardware is delivered to the polling place and physically set up. MBBs may have been preinstalled in the election hardware at election headquarters, or may be delivered

---

[116] *Hart Voting System System for Election Records and Verification of Operations (SERVO) Operations Manual Revision 42-62B,* Hart InterCivic, Inc., Part No. 6100-102, May 2006, p.31.
[117] *Id.*, p.17.
[118] *Id.*
[119] *See* section 5.5 for further discussion of auditability.

separately. Pollworkers at the polling place are responsible for pre-election processes, and going through the "polls open" process. This involves pushing the "polls open" button, entering the "polls open" password, printing a zero report and announcing the opening of polls.

The documentation available to polling place workers largely consists of the *eSlate Polling Place Election Day Reference Desk Manual* and the *eSlate Polling Place Early Voting Reference Desk Manual* ("*eSlate Desk Reference*"). These two documents are virtually identical, with the exception of the section on "closing polls" (election day manual) and "suspending" and "reopening" polls (early voting).

5.1.12 eSlate and DAU Voting

When voters approach the pollworker, they are given a print ticket with a voter access code. These access codes expire at a predetermined time—by default, 30 minutes after issuance—and when the polls are closed. The documentation correctly advises polling place workers to prevent Access Codes from being misused or unnecessarily expired. For instance, if there is a significant delay between getting the access code and being able to vote because of lines or inability to access an available eSlate, a live Access Code could expire, be lost, misplaced, or passed to another voter. The *Desk Reference* documents advise pollworkers that "voters should not stand in line with 'live' Access Codes."[120] This prevents unnecessary polling place confusion and expired tickets.

As voters cast their ballots, a CVR is written to the eSlate or eSlate DAU (or scanned into the eScan). The eScan records to an MBB, and the eSlate/DAU send the CVR to the JBC, which records them locally and writes them to an MBB. Thus, DRE votes are stored in three different places: The eSlate/DAU, the JBC, and the MBB. Additionally, an audit tape is printed, creating a fourth record. Print ballot votes are stored in three different places: on the printed ballot (which is stored in the eScan storage bin); as a CVR on the eScan's memory; and as a CVR on the eScan's MBB.

As the vote is cast, ballot images (the CVRs) and audit data are simultaneously written to the MBB—the same device. ("As voters cast their ballots, ballot images (Cast Vote Records [CVRs]) are written to the MBB as well as audit data associated with the election events.")

Curbside voting, which is not certified in California, involves assigning an access code to the curbside voter; then entering the access code & enabling the eSlate or eSlate DAU; then disconnecting the eSlate/DAU from the JBC daisy chain; then taking it to the voter who casts a vote; then returning it to the JBC daisy chain. At that point, the vote is recorded on the JBC and the MBB.

Troubleshooting instructions for the pollworkers and polling place support staff were not in all cases helpful. For instance, the *eSlate Desk Reference* documents, which are intended for use by pollworkers, have several solutions to what to do if the "poll close procedure" is initiated too early in the day. At two places in the "poll close procedure", it is possible to abort the closing process. However, if the polls have actually been closed,

[120] *eSlate Polling Place System Early Voting Desk Reference (System Version 6.2) Revision 6.2A*, Hart InterCivic, Inc., Part No. 6300-131, May 2006, p.39.

the documentation simply says, "If you see the Polls Closed screen before closing time and it is Election Day, call the Elections Office or Help Desk."[121] Unfortunately, the manual that the Help Desk will be using (the *System Support Procedures*) also says, "If it is Election Day, and you are on a Polls Closed screen, call the Elections Office or Help Desk." Further down in the page, the documentation says that the item has to be pulled. The formatting of the manual, however, makes it difficult to understand that these items are connected. This is the sort of problem that may be remedied in training; however, standing alone, the documentation is confusing here and elsewhere.

Troubleshooting documentation was also inadequate in other places. For example:

- The JBC has a contrast up and a contrast down button. Maximum/minimum specifications are established on "contrast down" so the JBC can't get too dark. Unfortunately, they aren't established for "contrast up", so the JBC screen contrast can be turned up all the way—so that the entire screen is a uniform light grey. Polling place workers who are unfamiliar with computer equipment, anxious or nervous, could have problems with this. Especially since "contrast up" and "contrast down" are not necessarily intuitive in themselves, and a user may need to hold "contrast up" for several seconds in order to bring contrast back to visibility. However, this problem was not addressed in the documentation.
- The eSlate and eSlate/DAU also present a user interface issue that affects both the polling place worker and the voter. The eSlate and eSlate/DAU offer a button to press "help", which flashes a small light on the JBC next to the indicator for that eSlate or DAU. This interaction was problematic in two ways. First, the flashing light seems unlikely to get the attention of the poll worker. The light is already on, indicating that the eSlate is in operation. When "help" is pushed, the light flashes on and off. The light is not very bright, and in a brightly lit polling place, is difficult to see already; the flashing is relatively unobtrusive. Second, on the voter's end, pressing "help" generates a message on screen for the user. The user is encouraged to press "help" again, or at least, not warned from not doing so. Unfortunately, pressing "help" a second time makes the flashing light on the JBC stop flashing. The voter, who has pressed help two times and is waiting patiently for assistance, may never be noticed. The documentation includes no information about this particular problem, and simply advises that election managers should maintain sufficient staffing levels at polling places to monitor the JBCs.[122]
- The printed text on the VVPAT cut off moderately long candidate names. For instance, we defined a candidate "Johnny Smartypants"; the VVPAT record showed the first fourteen characters, "Johnny Smartyp". Again, although this problem has been publicly documented,[123] it was not addressed in the user documentation available to the pollworkers or election officials and should really

[121] *Id.*, p.50; *eSlate Polling Place System Election Day Desk Reference (System Version 6.2) Revision 6.2A*, Hart InterCivic, Inc., Part No. 6300-132, May 2006, p.48.
[122] We note that this particular problem is likely best addressed with minor hardware and software modifications. For instance, use of a red/green LED at the JBC, and an overhead red light and warning to the user.
[123] *See* Proebstel et al., note 66.

be addressed in the design of BOSS so that adequate decisions can be made during election definition.[124]

In general the documentation lays out an ideal system, but with little information about how to handle problems or troubleshoot the system. When problems did occur, referencing back-and-forth throughout the documentation was often required. The documentation available to polling place workers (the *eSlate Desk Reference*(s) were often inadequate for troubleshooting, requiring recourse to *System Support Procedures* that would likely require a call back to technical support or election headquarters. Moreover, the troubleshooting guide sections of the *eSlate Desk Reference*(s) were organized alphabetically by topic, with no additional indexing by error message. For instance, the section labeled "CLOSE POLLS button"[125] says what to do "If someone has pushed the CLOSE POLLS button before closing time." However, the pollworker who looks at a JBC may not recognize that that is what is going on, seeing only an unfamiliar screen. The guide offers the advice, "If you see the Polls Suspended screen and it is an Early Voting day, …", but that is buried within the CLOSE POLLS button screen. This can lead to unnecessary confusion for the pollworkers and potentially impede the process.

5.1.13 eScan Voting

The eScan is a dedicated proprietary piece of hardware, with a built-in automatic feed scanner, a thermal line printer, local flash memory, a PCMCIA slot for the MBB, and two secure compartments for ballot storage. The eScan is intended to be used only with ballots printed in advance on paper of a specified weight and dimension. As with the JBC, the eScan should have zero-tapes printed as the last step before being deployed in an election.

In our walkthroughs, we attempted several times to run printed ballots through the eScan. Unfortunately, the documentation was unclear that the ballots printed "on demand" were in some way incompatible with preprinted ballots intended for use with eScan. Consequently, these ballots were generally unread by the eScan and the overly-aggressive feed mechanism of the eScan caused many of our test ballots to be mangled. The error messages during this process were unhelpful, as was the documentation. Indeed, only in the *Ballot Now Operations Manual* does it note briefly that these ballots are not intended for use in the eScan.[126] The election official, or pollworker, processing such a ballot would likely not have ready access to the *Ballot Now Operations Manual*. Unfortunately, virtually no information about the eScan is available in the *eSlate Desk Reference*, the primary resource for pollworkers. The primary troubleshooting guide for the eScan is in

[124] In fact, this is one of a number of cases where an issue was noted by the State Consultants but did not make it into the *Hart Use Procedures*. On page 7 of the Consultant's Report, they note: "It was discovered that a test "long candidate name" with 25 characters in the first name and 35 characters in the second name would not be displayed on the eSlate using a single column ballot. […] If this version of the system is certified this will need to be addressed in the use procedures." The use procedures contain no warnings about long candidate names.

[125] *eSlate Election Day Desk Reference*, note 121, p.48.

[126] *Ballot Now Operations Manual*, note 17, page 24, "The processing of paper ballots printed for an eScan is not described in this manual."

the *System Support Procedures*.[127] However, even here no information was available about what to do if the scanner feeder "eats" a ballot.

5.1.14 "Polls close" and "Polls suspended" Operations

Poll closing (and poll suspension) is done by the pollworker. On the eScan, the pollworker uses the console screen to close the polls, and on the JBC, the pollworker simply presses a dedicated "polls close" button. This button closes down the eSlates, turns any open access tickets to a "closed" status, and shuts down the ability to do some reports. Both the JBC and the eScan ask for a confirmation, and a confirming password. The pollworker fills out end-of-day reports, using information from the JBC/eScan reports, and then disconnects the JBC from its battery key and power. The MBB may be left in the sealed devices (JBCs and eScans) and transported to Rally or Tally stations. Alternatively, MBBs may be removed from the devices, with the MBBs and seals logged on a transfer envelope, and the MBBs transported to Rally or Tally stations.

When polls are suspended, rather than closed, the MBB is *not* removed from the voting device.

When closing an election on the JBC, the pollworker can print tally reports and write-in reports. However, these options are not available after the polls are closed. Closing the polls also decrements the "open access code" count and increments the "canceled access code" count. In general, to avoid unnecessary pollworker confusion, poll closing should generate more information, including a warning about the reports and options to print any reports the pollworker won't be able to print afterwards. Poll closing should also notify the pollworker that there are *n* open access codes, and that closing the polls will close the open access codes.

Poll-closing time may be configured in the ballot definitions in BOSS.[128] This causes a warning message if a user presses the close-polls button on the JBC prior to the time specified. This is a useful precaution, which should generally be implemented.

Neither the BOSS nor pollworker documentation is California-specifiic. The California Elections Code provides a uniform poll closing time of 8:00pm, although voters in line at that time must be allowed to vote.[129]

The documentation about the eSlate for pollworkers in the *eSlate Desk Reference* is minimal, with just the very basic "press this button"-level instructions. There is no information about the eScan.[130] However, the *System Support Procedures* include more information, including checklists for all devices.[131]

---

[127] *System Support Procedures*, note 22, eScan Device Troubleshooting Quick Reference (pp.184-186) and Troubleshooting Guide (pp.187-209).
[128] *BOSS Operations Manual*, pp. 118-119.
[129] California Elections Code § 14401.
[130] *eSlate Desk Reference Early Voting*, pp. 31-34; *eSlate Desk Reference Election Day*, pp.30-31.
[131] *System Support Procedures*, note 22, "MBB Processing and Election Night Procedures" (pp. 241-248; PDF pp. 247-254).

5.1.15 Rally Documentation and Procedures

The documentation for the Rally operation appears to describe normal operation adequately. We were not able to test the Rally-Tally connection in our walkthrough.. The lack of troubleshooting information in the Rally Operations Manual, however, suggests that if unpredictable events do occur, it would be difficult to deal with them. For instance, the *Rally Operations Manual* warns on page 60 not to use a recovery MBB made with SERVO in reading MBBs into the Rally database. However, it is unclear what the consequences of this might be: corrupting the database, or simply generating an error message.

The Rally documentation was also unclear in describing the basic setup, including, for instance, instructions for connecting MBBs to *Tally* PCs—instructions that were likely copy/pasted from the Tally documentation.

The procedures include an optional human phone confirmation that the number of MBBs read by the Rally station was equal to the number of MBBs transmitted to the Tally station at election headquarters.

Based on a review of the procedures specified in the documentation, Rally operations also raise auditability, security, and accuracy concerns, which are addressed on those sections.

5.1.16 Tally

Tally reads and tabulates results sent to it by Rally for preliminary results, and reads and tabulates MBBs from the polling places for final results. Once Tally finalizes the election, no further MBBs can be read.

In general, the documentation for Tally is clear and usable by election officials in normal operations. During the Doc Team's walkthrough, we were able to initialize a Tally election database, finalize a database, and view reports without difficulty, using the *Tally Operations Manual*.

Tally accuracy and reliability, security, secrecy, and auditability are discussed separately in those sections, or in conjunction with the Rally program.

5.2 Accuracy and Reliability

The accuracy and reliability of a voting system rely principally on hardware and software, with documentation and procedures used to verify the accuracy and reliability of the equipment, and to ensure that malfunctions are recognized quickly without interfering with the election. Reliability commonly refers to the proportion of time that a resource (e.g., a voting machine) is available for its intended use. Accuracy refers to the ability to correctly capture and record information without error.

The documentation that Hart provides generally assumes that the machines will be accurate. "Logic and accuracy testing" procedures are included. These tests are generally very clearly laid out for the user procedurally. However, they usually offer little explanatory information that clarifies how or for what the tests are testing. For instance, documents include considerable reassuring language ("triple redundant storage", "triple redundancy features"), which is not well-defined., Similarly, while the user can create a

"recount MBB" in SERVO that consists of all the records (CVRs, audit logs) from MBBs in an election, the documentation provides virtually no information about whether or not doing an automated recount actually verifies consistency and other properties of these records.

Additional discussion of potential security issues that may affect accuracy may be found in the *Security* section, below. *See also* the *Testing* section, above, and the *Auditability* section, below, for information about verifying and validating the accuracy of results.

5.2.1 Testing Procedures and Documentation

Hart includes well-defined procedures for a variety of tests: Acceptance testing, functionality testing, pre-deployment testing, logic and accuracy testing, and so on. These procedures are generally helpful for establishing facility with and functionality of the basic election processes.

When the systems are delivered to the purchaser (the county), the county must go through an acceptance testing procedure to verify the equipment is in good working order. The acceptance testing procedure includes (a) unboxing and checking receipt of equipment and supplies; (b) setting up and testing voting booths, JBC and eSlate voting units; (c) using SERVO to log serial numbers of JBCs and eSlates, write the signing key to the JBCs, set the clock in the JBCs, and verify firmware revisions in the JBCs and eSlates; (d) inventorying the serial numbers of booths, eSlates, JBCs, and booth caddies; (e) reconfiguring booths and JBCs for storage, and storing equipment (booths on caddies and JBC boxes on shelving); and (f) testing the eSlate (casting 20 ballots on each) and eScan (casting 50 ballots on each).

During Acceptance Testing, election staff are in charge of affixing self-adhesive serial numbers to the equipment.[132] While this is treated as a routine operation, the serial numbers are used throughout the lifecycle of the system for inventory control and processing. Consequently, maintaining control and accuracy during this process is important to ensuring that election hardware is uniquely identifiable and trackable.

Hart recommends performing functionality testing between election cycles to verify that the equipment is still operating and is election-ready; at least once a year is the recommended minimum, but more often is permitted.[133]

Polling place hardware needs pre-deployment testing, both *basic functionality testing* and *logic and accuracy testing*. Basic functionality testing requires verifying that the individual devices can power up and boot. Logic and accuracy testing requires testing the equipment in a test mode with cast ballots to make sure they record votes correctly.

EScan and JBC must run a "zero tape report" before the polls open to certify that no CVRs remain on those systems. When JBC and eSlate start up, they automatically print results of diagnostic tests. Ballot Now Election Report must be printed to serve as a zero report *before ballots are scanned*.

Tally's logic and accuracy testing procedures were covered in the *Systems Support Manual*, and also in the Tally Training Manual, which was not provided.[134]

---

[132] *System Support Procedures*, note 22, p.41, 43, etc. (PDF p.47, 49, etc.).
[133] *Id*., p.38 (PDF p.44).

Ballot Now requires accuracy testing; however, this procedure is covered in the Ballot Now Training Manual, which was not provided. Ballot Now testing must be completed by ten days prior to the election.

The eSlate requires Ballot Inspection and Verification (BIV) testing, using two test mode MBBs in BallotNow and eScan.

5.2.2 Recounts

The ability to do recounts is a critical component of ensuring a voting system's accuracy and reliability. Unfortunately, because we were not given the *Tally Software Training Manual*, with "Appendix G: Hart Voting System Recount Procedures",[135] we were unable to fully assess these procedures.[136]

Hart's SERVO application permits creation of recount MBBs from its local copies of voting system device memories. Recount MBBs may be generated for eScans, eSlates, or JBCs. According to the SERVO Operations Manual, these recount MBBs may be used in Tally to compare election results with the MBBs written by those devices and read into Tally. Unfortunately, this process is not described in the *Tally Operations Manual*. While a user could infer that one is to import the data from the MBBs, it is unclear whether that would involve initializing a second election, or using the existing election database. Using the existing one raises the risk that original files could be overwritten or appended.

5.2.3 Accuracy Issues in Rally

According to the *Rally Operations Manual*, it appears that although Rally captures CVRs from the MBBs,[137] it only sends "ballot counts" (an undefined term) to Tally. This is potentially problematic, since any tabulation problem in Rally would then be transmitted to Tally.

The *Hart Use Procedures* are internally contradictory on this point. Section 10.3 ("Security Procedures for Central Processing") states that

> The MBBs from the Rally station(s) are delivered to Central Tabulation, they are ready again into the Tally System. The unique serial number in the MBBs is used to prevent duplicate storage of the information in the MBB.

Directly contradicting this, section 7.2.2 on Processing Vote Reports states that,

> Since the CVRs from the MBBs read at the Rally station(s) are uploaded to Tally via an intranet or dial-up connection, they do not need to be read again into the Tally system. The unique serial number in the MBBs is used to prevent duplicate storage of the information in the MBB if an MBB from a Rally station is inadvertently read directly into Tally.

Other Hart documentation does not clearly address this issue. The obvious failsafe would

---

[134] The *Hart Use Procedures,* p.18 et seq., specifies Tally Training Manual 6300-005 62A, "Logic and Accuracy Testing Procedures".
[135] *Management & Tasks*, note 7, p.26 (PDF p.32).
[136] The procedure is apparently also covered in a "Tally Operator Training Course".
[137] *See* Appendix B, Rally log, *Hart Voting System Rally Operations Manual Revision 23-62A*, Hart InterCivic, Inc., Part No. 6100-114, March 2006.

be to have Tally verify the MBBs directly, in line with Section 10.3 of the *Hart Use Procedures*. Section 7.2.2 should be revised to reflect this understanding.[138] Moreover, the Tally read should not simply recognize a duplicate MBB and refuse to read duplicate results into the database; it should *use* the direct read from the MBB to verify the Rally-transmitted results.

Note that this issue also raises the statutory concern of "official" results.[139] If, as seems to be the case, the Rally communications are fed directly into Tally and never verified or replaced, they become the final counts unless a recount is requested.[140]

We also noted that the documentation warns users not to "resend the MBBs to the Tally PC" unless instructed to do so by Election Headquarters. However, no information that we could locate explains how to tell if this has happened, what the consequences are of doing so, or how to undo it if it is done.[141]

5.3 Security

Security of voting systems is essential to prevent tampering with, accidental alteration of, or unauthorized disclosure of election results. Security is implemented through a combination of hardware, software, and procedural mechanisms. Documentation should adequately describe the hardware and software security mechanisms to ensure that users understand and are able to utilize those mechanisms correctly. Documentation should also set forth clear and appropriate procedures to compensate for any security holes in the hardware and software applications.

Hart documentation generally provides detailed procedures for security, and supporting documents to facilitate adoption of security procedures. In some instances (detailed below), we found the security procedures inadequate. Also as described below, the documentation frequently fails to highlight security-related concerns in use procedures.

5.3.1 Documents Relevant to Security

The bulk of Hart's treatment of security occurs in the *Hart Use Procedures*,[142] a redundant *Security Procedures* document[143] and in the *Hart Product Description*.[144]

The *Hart Use Procedures* treat security issues from section 10 of the use procedures template: physical security (10.2), logical security (10.2),[145] central processing security (10.3), polling place security (10.4) and audit trails (10.5). In general, the *Hart Use*

---

[138] Section 7.2.2 also misstates the communications. Rally-to-Tally connections need not be restricted to an intranet. According to the documentation, only a direct IP connection with SSL is necessary; this configuration would work on any TCP/IP-based network (i.e., the Internet).
[139] *See* discussion in note 31.
[140] *Tally Functional Specification Revision 43-62C*, Hart InterCivic, Part No. 6000-047, April 2006: "Tally shall receive sufficient information ..." p.56. Sec 3.19.3.
[141] *Rally Operations Manual*, note 137, Ch. 3 p.70.
[142] *Hart Use Procedures*, note 2.
[143] *See* "Security Procedures - HART -.pdf". This document is basically a short (4 page) overview of security procedures implemented throughout the system. The document is taken almost *verbatim* from the Hart Use Procedures, and includes little additional useful information.
[144] *See Hart Product Description*, note 38.
[145] This might be more properly termed "Software Security".

Procedures includes only high-level information about security procedures, and then largely points to the places in the documentation that detail functionality related to security procedures (e.g., how to manage tamper-proof seals and permission levels/password requirements). The list of computing services in section 10.2 of the use procedures (largely telecommunications and networking services) that must be disabled and remain disabled on HEMS computers do not include any index references. Sections on storage and delivery procedures, access controls in HEMS software and eCM security do not include any index references to locations where they are treated in more detail.

The *Hart Product Description* includes four pages of material entitled "Computer Security and Recovery".[146] This content mostly consists of "tips and techniques" useful for maintaining a secure elections environment. Perhaps the most useful advice here is a whole page about password security, where Hart details common pitfalls associated with passwords that are known to make systems much less secure.

Ideally, a "Security Procedures" document would include a complete set of security protocols and procedures, with short instructions, and indexing to more complete protocols and procedures throughout the system documentation. For instance, system warnings scattered throughout documentation should be indexed here.

5.3.2 MBB Chain of Custody

MBBs are a critical component of the election process. Ideally, they should be clearly labeled, inventoried, and tracked. They should also be protected from misuse or accidental treatment. The *Hart Use Procedures* mandate that a strict chain of custody be maintained for ballot media. Hart offers a number of paper-based logs that facilitate tracking of ballot media and election devices.[147] However, Hart's user manuals and procedures here, as elsewhere, fail to contextualize guidelines with the explanations and rationales. The *Management & Tasks* Chapter 2, "Election-Related Management", includes the information one would need to maintain chain of custody in relevant checklists. For instance, the "Election-Related Tasks Checklist" lists "Starting the equipment Serial Number Logs" and "Starting the Ballot & Seal Certificate documents" in a list of eleven items.[148] These refer to the *System Support Procedures*, which include references to and samples of the paper-based audit logs.[149]

The procedures do therefore incorporate the necessary pieces of the *Hart Use Procedures* with respect to chain of custody maintenance, although the information is not always as usefully or clearly highlighted as it should be. For instance, although the *System Support Procedures* and *Management & Tasks* manuals include checklists and references to the paper-based audit logs, the *SERVO Operations Manual*—which includes instructions about formatting the election equipment—includes neither references to the manual logs, nor admonitions about ballot media security or tracking.

---

[146] *Hart Product Description*, note **Error! Bookmark not defined.**, pp.27-30.
[147] *See, e.g.,* "Voting Device and MBB Tracking Log", *System Support Procedures* (PDF p.331); "MBB Transfer Envelope" labels, *System Support Procedures* (PDF p.294). *Management & Tasks*, "Appendix G: Election Logs" lists all the support procedures (PDF pp.129-130).
[148] *Management & Tasks*, p.21, PDF p.27.
[149] *See, e.g.*, Step 9 of "eSlate Booth Preparation Instructions", *System Support Procedures*, p.90 (PDF p.96) ("Secure VBO with a wire seal, log security seal number").

We also note that in the TTBR configuration of equipment, the MBBs provided by Hart to the Secretary of State for testing purposes were labeled inconsistently and not clearly about which end fits into the device in which direction. This could lead to pollworker or election officials trying to force the device, harming the pinning, or being too tentative to actually insert the MBB. It is unclear to us whether these labeling problems would be typical of the system as used in the field.

5.3.3 eCM Key Security

The procedures for securing the eCMs (the USB keys) are critical to ensuring the security of the overall system. This is recognized by the *Hart Use Procedures*, which state that "The eCMs should be closely managed. The number of eCMs being used for an election and their PIN(s) should be logged in a secure election. … eCMs should be stored in a secure location, separate from election MBBs."[150] Unfortunately, this guideline is vague, and the Hart documentation gives little assurance that the goals of this use procedure will be met.

eCMs can be recreated from preexisting eCMs or from a .eCM file, using eCM Manager and the PIN. Since eCMs and eCM control are critical to the security of the system, it is critical that all creations of eCMs be logged in an audit log. Unfortunately, eCM Manager has no such logging capability.

Moreover, the Hart procedures discourage additional security procedures by noting that "You can also increase security by creating new signing keys and rewriting eCMs at regular intervals (e.g., with each election, annually or quarterly), but this also adds a level of complexity to procedures."[151] They make similar comments about unique PINs for each key.

The procedure says to store the labeled eCMs in a secure location, but says nothing about the .eCM file. This file is stored on both the eCM Manager computer, and (recommended by the procedures) on a backup CD.[152]

However, since the eCMs can be recreated so loosely, concerns arise about creation of the keys without eCM Manager—for instance, simply by using the operating system to copy the files from one USB key to the other. Reproduction outside of eCM Manager depends on the security features of the Spyrus key, to which the Documentation Review Team did not have access. Some programs that require eCM access are intended to be run in a distributed fashion (e.g., Ballot Now and Rally). If eCM Manager is *not* required to reproduce eCMs, then this is a procedural vulnerability that could expose eCMs to unauthorized reproduction.

Password specifications are in at least one place inconsistent. For example, throughout the documentation it species passwords or "PINs"—really, a password or passphrase—of 6 to 12 characters. In Rally, the password specs require "6 to 12 lowercase characters".[153]

---

[150] *Hart Use Procedures*, p.48.
[151] *Management & Tasks,* note 7, p.42 (PDF p.48).
[152] *Id*., p.43 (PDF p.49).
[153] *Rally Operations Manual*, note 137, Chapter 8 "Managing Rally Users", p.99.

5.3.4 Role Definitions

Role assignments and role definitions are used to secure access to critical functions in a software program and to prevent inadvertent error that might occur when a user has privileges they may not need to complete their tasks. Good role definition creates narrow roles for particular task functions, and limits access to functionality other than necessary for that role. Documentation and user interface design guides how these functions and roles should be presented to the user to facilitate use of role definitions and role assignment capability.

The Hart system appears, from the documentation, to establish a reasonably limited number of defined roles to maintain access to critical components of the HEMS. Within each of the subapplications, a limited number of administrator and user roles are defined with access permissions. The operations manuals for the individual software programs describe the available roles and their functions, permitting administrators to make informed decisions about how to assign roles.

As in other aspects of Hart documentation, the rationale that might guide such choices is poorly or not at all explained. For instance, the *BOSS Operations Manual* simply describes the mechanics of establishing and changing user permissions and roles, with no warnings or cautions about the implications of doing so and no guidance as to why it is important to segregate users of the system and compartmentalize privileges. The only document that appears to give direct advice in terms of user roles and privileges is the *Hart Product Description* which includes a paragraph entitled "Never Give Administraion Privileges"; this section advises jurisdictions to only use administrative privileges as needed and to never give them out to "regular operators" or "lay citizens".[154]

The *eSlate Management & Tasks Procedures Training Manual* goes into much more detail in terms of outlining the various types of users allowed and the actions they can perform. When compared with the exceedingly complicated role-management in Sequoia's WinEDS,[155] Hart's role administration seems to be relatively straightforward and doesn't seem to pose the same kinds of risks.

However, there are important issues with this documentation. First, as we pointed out before, the documentary content with respect to user roles is largely descriptive with little discussion of why certain practices might be better than others. Also, two applications, Rally and SERVO, seem to have only one role available, which significantly impacts the procedures surrounding their use. In addition to physical and logical security, Rally and SERVO users must also be experienced and trusted individuals.

5.3.5 Security Issues in Tally Documentation and Procedures

Tally security procedures are based primarily on controlling physical access to the Tally equipment and using the eCM for access to the program. Because Tally is a back-office application, not run in a networked configuration, it is as secure as the local access procedures establish. However, eCM keys are (as discussed in the eCM section) a point of vulnerability. Moreover, any security of Tally ultimately rests on security of

[154] *Hart Product Description*, note 38, p.28.
[155] *See Sequoia TTBR Document Review Report.*

interfacing applications. Consequently, polling place or MBB problems can compromise the security and accuracy of the Tally database. In particular, Tally's interface with Rally appears to be a weakpoint (discussed below).

Tally's audit logs are discussed in the audit section, particularly with respect to the audit logs for the Tally Vote Adjustment feature.

5.3.6 Security Issues in Rally Documentation and Procedures

Security concerns arise from the distributed nature of Rally operations and the network transmission of election data. Rally's security is primarily based on (a) use of the eCMs to control access to the Rally application; (b) procedures that control physical access to the Rally machine; (c) a "Rally certificate" which is generated in Rally and used by Tally to validate the machine; (d) a "Tally certificate" which is generated in Tally and used by Rally to secure and authenticate communication between Rally and Tally; and (e) procedures in configuring Windows' network/telecommunications access on the Rally machines. We review these issues in turn.

5.3.6.1 eCMs

The use of the eCMs to control access to the Rally application is helpful in securing the election and should eliminate some potential attacks. For instance, without an eCM, a user could not gain access to the Rally database to change its security certificate and prevent uploading of results to Tally. However, it also increases the risk of other attacks by requiring that the eCMs be taken out of election headquarters and further exposed. *See* the eCM Manager / eCM section for more discussion of the need to secure eCMs. It also relies on the level of security enjoyed by eCMs, which, as discussed previously, appears insufficient.

5.3.6.2 Physical Security Procedures

Procedures establishing physical controls over the Rally machines are sparse. Only the *Management & Tasks* manual has any reference to such procedures, stating in "Chapter 3 Software Administration Tasks" that "It is Recommended that the User Currently Logged In ... Stay at the computer while running the application, Exit the application if s/he steps away from the PC." This is not sufficient, since access to the Rally computer could permit alteration to the Rally database. Since Tally automatically polls Rally periodically, a user could alter the Rally database after an MBB is loaded and before the polling period. Furthermore, if the Rally application is closed, Tally can't connect to it.

5.3.6.3 SSL Certified Transmissions

Rally generates an SSL certificate that is input into Tally to prevent false Rally stations from sending data to Tally. Similarly, Tally generates an SSL certificate that is input into Rally; this prevents Rally from responding to false Tally machines. We had no technical specifications for Rally, but the functional specification for Tally notes the SSL certificate, and user documentation suggests resetting Rally certificates periodically. The SSL certificate protects the data while in transmission. This is particularly important for ensuring that election data is neither intercepted nor compromised in transit.

5.3.6.4 Network/Telecommunications Access

Because Rally operates on machines with modem or ethernet network access, it is imperative that this access be controlled. The Rally instruction manual includes information about configuring Windows network access.[156] However, it is unclear whether the instructions are detailed enough to result in the level of operational security required. For instance, in defining "Incoming TCP/IP Properties", the documentation explains that the "from" address should be the Tally's. The documentation says nothing about the "To" address, and the default is a range of IP addresses. Moreover, the documentation fails to specify that *other* Windows networking connections should be entirely disallowed. The default functionality of Windows is to permit creation of multiple "network connections"—a package of network settings. If incoming dial-up or network access is enabled, users could access the machines to read or tamper with the Rally database file, especially if the user configuring modem access on the Rally computer fails to notices that one of the "Allowed Users" in the Network Connection Wizard is checked (which would mean that user can log-in to the computer over the modem connection). We recommend developing a comprehensive checklist of network/telecommunication settings in the documentation.

5.4 Secrecy

The California Constitution,[157] California law[158] and the VSS[159] require that a voting system ensure that voters' individual voting choices remain secret, while voter identification and record of voting is a public record. Ensuring that the identity of each voter who cast a ballot in an election are accurately tracked, and the entire content of each voter's choices are accurately processed, while simultaneously ensuring that those two pieces of data may not be associated, is the goal of secrecy requirements. Documented procedures as well as hardware and software measures ensure that the contents of the ballot are accurately tabulated while remaining secret and unlinked to each voter's identity.

In general, the Hart procedures specified in the documentation adequately protect the secrecy of voter information. Below, we highlight issues of particular concern or interest.

5.4.1.1 Access to Polling Booths

Access to the polling booths is controlled with a random four-digit access code, which is not tied to voter information in the system. The Source Code team found that the code generation process is vulnerable to attacks and suggested technical mitigations.

---

[156] *Rally Operations Manual*, note 137, pp.27-31

[157] California Constitution, Art. II, Sec. 7, "Voting shall be secret."

[158] Cal. Elec. Code § 19205(b) (a voting system shall "preserve the secrecy of the ballot").

[159] VSS Vol. I, § 2.4.3.1 ("[A]ll systems shall … [p]rotect 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.").

The *Hart eSlate Desk Reference* appropriately admonish poll workers to protect the voter's vote choice secrecy, and provide guidelines to "stand beside the privacy screen to protect the voter's secret ballot."[160]

5.4.1.2 Ballot Barcodes, CVRs, and Audit Logs

The Hart Use Procedures disallow the use of unique serial numbers on ballots and embedded in barcodes in order to protect the secrecy of voter information.[161] However, other types of information may create an identifiable profile. For instance, if a ballot included booth ID number and time of voting, this information could be combined with security camera feeds to disclose voter identity information. Similarly, voter sequence information may be combined with reviews of ballots and ballot sequence information (as provided by VVPAT printer rolls) to determine voter information.

The Hart VBOx printout includes a barcode. The documentation does not affirmatively indicate that voter-specific information is not stored in the barcodes when the Hart Ballot Key is disabled. Booth ID information identifying the eSlate booth ID can pose an even greater threat to voter confidentiality, since there would likely be few or only one DAUs at any given polling place.

Curbside voting is not certified for use in California because of the present lack of the VVPAT. However, audit logs could present an issue here, since curbside voting is likely to have an identifiable delay signature in the removal of the eSlate from the booth, entry of the access code into the eSlate, completion of balloting, and reattachment of the eSlate to the booth (which writes the CVR to the MBB).

5.5 Verifiability / Auditability

Conducting audits permits verification of an election, and helps to ensure security and secrecy. Post-election audit activities encompass a myriad of important processes, from cross-checking signatures in voter registration poll books, to investigation of anomalies to spot checks on vote counts, equipment and internal processes.[162] Audits and election challenges rely on the ability to recount votes and also to inspect auditing data to understand what may or may not have happened during an election. There are two aspects of auditing that we will address in this section: issues with audit logs and with the Hart system's support of the 1% manual tally.

5.5.1 Hart System Support for the 1% Manual Tally

A key part of the California Electoral process is the 1% manual tally.[163] The manual tally occurs during the canvass period and involves a manual recount of ballots from 1% of

---

[160] *eSlate Desk Reference*, p.22.
[161] *Hart Use Procedures*, note 2, p.15.
[162] *See, e.g.*, *Collaborative Public Audit of the November 2006 General Election Report of the Public Monitor of Cuyahoga County, Ohio*, Apr. 18, 2007, *available at:* http://urban.csuohio.edu/cei/public_monitor/cuyahoga_2006_audit_rpt.pdf.
[163] The 1% manual tally is defined in CA Elec. Code 336.5: "'One percent manual tally' is the public process of manually tallying votes in 1 percent of the precincts, selected at random by the elections official, and in one precinct for each race not included in the randomly selected precincts. This procedure is conducted during the official canvass to verify the accuracy of the automated count."

precincts, randomly selected (as well as additional precincts for races that were not selected in the initial sample).[164] Paper ballots and VVPATs[165] are manually tallied and compared to the electronic tallies stored in the election database. The time period for the canvass is a relatively short 28 days. Features of the voting system can significantly affect the efficiency, transparency and integrity of this process.

One documentary anomaly relevant to the 1% manual audit is common for each vendor in the TTBR. Each set of use procedures for the three vendors examined in the TTBR specify that the 1% manual recount should begin "within fifteen days after every election".[166] This is no longer correct. Such a requirement previously existed, but it was repealed in 1998.[167] This language is not included in the California Use Procedures template, so it is unclear where it comes from and how it comes to appear in the use procedures document for each vendor.[168]

Hart provides very little documentation about how users (election officials) might conduct the manual tallying process using the Hart system. The *Hart Use Procedures* have a total of 4 paragraphs (Section 8.6) that cover the manual recount process and most of that content consists of references to California election law. There is no advice as to counting methods, whether or not and how to count VVPAT ballots, or what might cause discrepancies and how to investigate them using the Hart voting system's tools and audit logs.

There is evidence that the Hart's Tally database reports are not well suited for the manual audit. In the logs of the volume testing incidents which we received, incident number 24 says, "Per vendor, Tally still cannot report vote results in the granularity required for the SSOV [Supplement to the Statement of the Vote]. (jurisdiction must export data and use an alternate tool like Excel or Fusion[])." This comment suggests that the Tally software does not seem capable of reporting results along all ballot types and/or per precinct, the level of detail needed to manually tally each ballot type per precinct.[169] In addition to this being an issue with the SSOV, it will also cause problems with the 1% manual tally.

If a discrepancy is identified during the manual tally, it is critical that clear procedures exist for escalation depending on whether or not the discrepancy is explainable or unexplainable. In the case of unexplainable discrepancy, vendors should include detailed

---

[164] CA Elec. Code Section 15360.

[165] For DREs, the VVPAT must be used in the manual tally. CA Elec. Code Section 19253.

[166] *See Hart Use Procedures*, note 2, p.38; *State of California Procedures Required for the Use of the Diebold Election Systems*, California Secretary of State, November 2005, p.57, *available at:* http://www.sos.ca.gov/elections/voting_systems/ca_avtsx_use_procedures_11_14_05.pdf; *Voting System Use Procedures for California*, California Secretary of State, February 2006, p.9-1 (PDF p.79), *available at:* http://www.sos.ca.gov/elections/voting_systems/sequoia_proposed_use_procedures.pdf.

[167] Between 1994 and 1998, CA 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 in 1998 as part of a reorganization of the California Election Code (1997 Cal SB 627; Stats 1997 ch 1073).

[168] We understand from the revision history of the *Hart Use Procedures* that use procedures for a vendor are approved after feedback from Secretary of State staff.

[169] We were unable to cast the full range of ballot types during our walkthrough to say anything more definitive through our own experience.

suggestions on how to use their tools and audit logs to narrow the range of possible sources of discrepancy. This will allow the jurisdiction to efficiently resolve discrepancy and conclude such investigations without impacting other activities that have to be completed during the 28-day canvass period

5.5.2 Issues with Audit Logs

Audit logs are recorded throughout the Hart Election Management System from both election devices and election software. These logs permit elections officials to view election-events that occurred on equipment or software, in order to verify, reconstruct and diagnose election events.

Hart InterCivic generates numerous audit logs. Unfortunately, the eCM Manager, a key security-related application, does not generate any audit logs. Moreover, Hart's documented procedures do not fully take advantage of the audit logs, leaving election officials to determine the best use for themselves.

5.5.2.1 Available Audit Logs

- The principal polling place devices each produce audit logs, including JBC audit logs; eSlate audit logs; and eScan audit logs;
- Ballot Now produces several audit logs—the Election Database Audit Log; the Security Database Audit Log; the Filtered Election Database Audit Log; and the Filtered Security Database Audit Log;[170]
- Most, but not all, of the software applications—BOSS, Rally, Tally, and SERVO—produce audit logs. Documentation does not reflect any audit logs from *eCM Manager*.

5.5.2.2 Usability of Audit Logs

We identified two kinds of potential problems with the Hart audit logs. First, the documented procedures do not always effectively use the audit logs. Second, the audit logs themselves may be placed at risk by some procedures within the Hart InterCivic system.

The usability of the audit logs themselves was out of scope of this review. Ideally, the user could check properties of individual audit logs as well as logical integrity across multiple audit logs. Those processes are unclear or nonexistent in the current Hart system. However, although not a comprehensive review, we discuss below some instances where auditing information seemed insufficient, or documentation did not adequately describe the available audit logs.

5.5.2.2.1 Use and Interpretation of Audit Logs

The documented procedures do not take advantage of the audit logs. For instance, while the *Tally Operations Manual* includes a section about its Audit Log,[171] there is no information included about when the Tally audit logs might be useful. One such time

[170] *Ballot Now Operations Manual*, note 17, p.25; pp.219-232.
[171] *Tally Operations Manual*, p.116.

might be after tabulation using Rally: the Rally audit logs and the Tally audit logs could usefully be compared to ensure that they match. A mismatch might suggest that a device polled Rally, disguised as an authorized Tally computer; or that the Tally computer failed or was blocked in retrieving CVRs.

Additionally, effective use of audit logs is sometimes hampered by poor documentation of their contents, what the items logged actually are, and the significance of those items. For instance, SERVO lists the Audit Log contents; these are documented in the "Audit Search Report" section of the *SERVO Operations Manual* (pp.132-134). Unfortunately, while the JBC, eScan, and eSlate record numerous auditable events (64, 46, and 47, respectively), these are not defined. Some are obvious (e.g., "VBO Paper Low"), but others raise questions and are not well documented elsewhere (e.g., "Encoded system failure file name"). Inadequate documentation of audit logs may render auditing difficult if not impossible, and certainly much more laborious than it should be for elections officials.

5.5.2.2.2 Procedural Risks to Audit Logs

Audit trails from election hardware are written to the MBBs and to the election hardware memory. The audit trail on the MBBs is read by the Tally systems, and the audit trail stored on the hardware memory is read by the SERVO systems.

If an MBB is compromised prior to being read by Tally, the audit trail for that MBB is lost. Since it is unclear from the documentation whether the actual audit trails are sent from Rally to Tally, the MBB audit trails may be at risk if stored only in the Rally databases, especially if the Rally databases are treated as "unofficial" or evade the comprehensive backups recommended for Rally.

Second, the audit trails from the devices may be lost by accident when resetting devices with SERVO. We observed that when resetting devices with SERVO, the system provides no warning or confirmation for "reset". Moreover, it retains the "reset" checkbox when moving from one device to the other. When one device (such as a JBC) is disconnected and another is connected, SERVO automatically resets the next device. This facilitates the rapid resetting of multiple devices. Unfortunately, however, "reset" and "backup" are part of the same user interface widget. A likely use scenario is the election official user who wants to connect a JBC and just backup the contents of the internal memory, then disconnect it; and then repeat the same procedure on the next device; and so on. This user must make sure that "reset" is unchecked after connecting—or the device is automatically reset *without* backing up. Particularly if the user combines backup and reset operations, it would be very easy to accidentally reset without backing up. This could significantly affect the creation of auditable backups, simply through poor user interface design.

The issue above should have been included in the *Hart Use Procedures* but is not. The State Consultants Report warned as much, noting that this had remained unchanged from system 6.1

> "As in the previous version of the system, when in the Backup and Reset Window of the Servo application, the 'Reset' button has no second chance warning the user. […] The use procedures need to address this, and we suggest providing a

second chance warning or a default setting to always back up data in future releases."[172]

However, the use procedures simply point to the *SERVO Operations Manual* and the *Support Procedures Training Manual*.

This problem is partially mitigated by including the SERVO "backup" features in post-election procedures. So, if election official users properly backup during a preceding election, the issue won't be a problem during reset for the next election. However, since the user interface is the same for both features, any backup process runs the risk of this user interface confusion. A user could easily reset while backing up, eliminating the possibility of using that device for later recounts. Moreover, the user operations manuals sometimes confuse the issue. For instance, the *SERVO Operations Manual* notes that "If the eScan, JBCs, and eSlate have been used in an Election, the Election data stored in them are backed up into an Event prior to the reset."[173] This implies that the backup is automatic, which it is not. Rather, procedures must be established to do the backup, and it is a manual process.

5.5.3 Rally and Tally Auditability

The Tally database is intended to act as a comprehensive election database for auditing and reporting functions, including all CVR and audit trail information from all MBBs. However, this is not the case when Tally is used in conjunction with the early election return program, *Rally*. When Tally-Rally operations are enabled, Rally reads the MBBs, and Tally polls Rally for the summary results. Rally maintains its own election database of MBBs read in Rally, and the Tally election database does not include that information.

This issue is a particular concern, since California law prohibits transmitting "official results" over public telecommunication lines.[174] Since the Rally aggregated results are not verified or cross-checked by Tally access of the MBBs, the Rally results are arguably "official" for that polling place or MBB. However, Rally may not meet the definition of a DRE.[175]

Auditability concerns arise in Rally regarding both its own internal audit, and its handling of the audit information from the MBBs.

5.5.3.1 Rally's Internal Auditing Features

Given that the security issues with Rally largely arise outside of the Rally application itself, Rally's internal auditing features are unlikely to capture the most serious potential events. However, for tracking the normal operations of the program, the audit log is reasonably informative and well-documented. For instance, the sample audit log included in the Rally Operations Manual includes the log items "Application login"; "Connection established"; "MBB transmitted"; and "Connection terminated" in rapid succession; these

[172] *State Consultant's Report,* note 73, pp.5-6.
[173] *SERVO Operations Manual*, note 116, p.22.
[174] CA Elec. Code Section 19250(g): "A direct recording electronic voting system shall not be permitted to receive or transmit official election results through an exterior communication network, including the public telephone system."
[175] *See* note 27.

descriptions make it apparent that they relate to a Tally connection.[176] While the "additional detail" information is oblique, the codes can be interpreted with the use of Table 4-3, "Audit Codes," in the Rally Operations Manual. For instance, the audit entry "MBB Transmitted", with an activity code of "42", lists "5" in the Additional detail column. This is ambiguous; it could mean 5 CVRs; 5 MBBs; the MBB ID of 5; or something else. The audit entry "MBB Processed" lists "5 - 11" in its additional detail. However, the Audit Codes table defines both these critical pieces of information. The "5" for "MBB Transmitted" refers to the MBB ID, and the "5 - 11" for "MBB Processed" describes both the MBB ID and the number of CVRs.

5.5.3.1.1 Rally's Processing of Audit Data from the MBBs

Rally's processing of audit data from the MBBs poses two significant problems. First, it appears from the documentation that Rally does not transmit the full set of CVRs and audit logs to Tally. Second, resetting Rally or restoring archived Rally files overwrites the current database file (mmbtrans.db), but use of the software-based archiving system in Rally is labeled as "optional", and relies on user file management skills. Rally's processing and securing of this data is a particular concern, since it appears that neither Hart software nor Hart procedures require any reading or verification of the original MBBs by Tally, once Tally has received the results transmitted by Rally.[177]

According to the *Rally Operations Manual*, Rally captures audit entries from MBBs.[178] However, it doesn't appear from the documentation or audit logs that Rally transmits this information to Tally. Our review of the audit logs shows entries from transmission of MBBs, but no entries or option for transmission of audit information. The "System Architecture" in *Rally Operations Manual* (p.17) similarly shows Rally sending "ballot counts" to Tally, but no auditing information.

Given what appears to be a failure to communicate auditing data to Tally, it is particularly important that the Rally database remain secure or that there be a process for ensuring that Rally-read MBBs are subsequently uploaded into Tally. Unfortunately, however, the archiving procedures established in the documentation do not facilitate security. In Rally as in its other EMS programs, Hart recommends and facilitates a number of backup options. Unfortunately, here as elsewhere, Hart relies on the user's knowledge about file management. Rally stores all its election data in one file, mbbtrans.db.[179] This database can be wiped out by two processes in Rally, reset and recover. Unless the mbbtrans.db file has been archived properly, the data may be lost from Rally. (While the original data can be reconstituted from the MBBs or original devices.) *Management & Tasks* references the Rally Archiving process,[180] and the *Rally Operations Manual* details the "archiving" procedure, which is described as "optional". In the "reset" section, it also warns users "IMPORTANT!" to archive the Rally database

---

[176] *Rally Operations Manual*, note 137, "Rally - Internal Audit Report" (PDF p.109).
[177] Although the *Hart Use Procedures* specify this in one place, note 2, p.49, they are contradicted elsewhere in the document
[178] *Rally Operations Manual*, note 137, Appendix B, Rally log.
[179] See, e.g., *Rally Operations Manual*, note 137, p.91: collects CVRs; Chapter 5 Rally Archiving; Chapter 1 "Rally Station Setup" pp. 43 et seq
[180] *Id*., p.60 ("Rally Database Management").

file "if necessary", and the Rally program reset command offers a confirmation box. The procedure, it turns out, essentially replicates a Windows file management exercise, in which the must user browse to select the file to archive; browse to find a location to save the file; and provide a filename. This procedure thus relies on user attention to detail, and user filenaming and file management skills.

5.5.3.1.2 Archiving

Throughout the Hart EMS documentation, users are recommended to backup or archive their data. Several of the applications even have integrated backup programs that facilitate this process. Unfortunately, whether integrated into the software, or handled simply through recommending to users that they backup data, Hart fails to explain to users two major issues with this method of backing up—both implicating security.

The first significant issue is the general lack of system control in the user interface over backup files and filenaming. Whether the application includes an integrated "archive" module or not, the user is expected to specify file location and filename for the backup copies. This is asking for trouble, since many users have only a modest grasp of file hierarchies or how file hierarchies work, and can lose or overwrite existing files. Even sophisticated users who well understand file systems can, working in haste or when tired, overwrite a preexisting file.

The second significant issue is the potential security risks from proliferation of uncontrolled or even lost archived datafiles. The Audit Logs includes back-up information, including filepaths,[181] which permits some control over the creation of the backups from Rally. However, it appears that the archive files are simple database files, which can easily be manipulated from within the Windows file system. This permits creation of uncontrolled archives (really, copies of the application's database), and accidental moving or deletion of archive files, rendering the Audit Logs' information less useful.

Ideally, the integrated archive features would create an obfuscated copy of the datafile, uniquely numbered, and read/write-protected. Recovery from archive would provide significant information about the archive to the user for confirmation, and also offer an opportunity to archive the working dataset at the same time.

5.5.3.2 Inadequate Audit Logs

While a comprehensive review of the adequacy of the audit logs was out of scope, we did observe some issues with the audit logs.

5.5.3.2.1 eCM Audit Logs

The eCM Manager does not appear to audit creation of new eCMs. Since controlling eCMs is key to maintaining security throughout the entire election process, this is a significant failure of auditability. Consequently, new eCMs can be generated through eCM Manager (either directly from the locally-stored .ecm file, from a backup .ecm file, or by copying from an existing eCM). The creation of uncontrolled eCMs can expose the entire Hart EMS.

---

[181] *See, e.g.*, *Tally Operations Manual*, Chapter 4 "Reports" ("Audit Log", pp. 116-118).

While Hart recommends maintaining a manual log of this process, instances of using the software to create new eCMs should also be automatically logged. While this wouldn't prevent duplication of the eCMs through other means, in conjunction with close security for the eCMs themselves, it would create significantly more control over this significant entry point into the system.

5.5.3.2.2 Tally Audit Logs

The audit logs for Tally Vote Adjustment were a particular concern, since Vote Adjustment is not logically constrained. The state consultant's report noted that a Tally administrator can adjust vote totals, without restriction as to basic mathematical relationships between vote totals and the number of ballots cast.[182]

Unfortunately, the audit logs documented in Tally User Documentation will record this only as "Manual Votes"[183] These include audit entries:

- 850 Adjusted Precinct/Split Precinct ID, Precinct/Split name, Source Type
- 851 Adjusted Contest Name Contest ID, Contest Title
- 852 Adjusted Option Name Option ID, Vote Adjustment Option Title

It is unclear whether this actually records total number of adjustments. The adjustments window in Rally permits, for example, subtraction or addition of multiple votes at once. Audit information should reflect the total number of votes added or subtracted, as well as the contests and options selected.

6 Conclusion

After reviewing the Hart system and user documentation, we conclude that it generally documents and facilitates running a simple, problem-free election. We are less sanguine about the ability of the documentation to quickly and readily provide solutions to address the wide variety of real-time election difficulties that might crop up. Additional user support documentation would facilitate this, including comprehensive indexing and references. In particular, more mid-level documentation that integrates the Hart system-specific steps and the California-specific *Hart Use Procedures* would ensure that critical procedures and precautions are not overlooked.

Auditing features should be fully explained and, as importantly, demonstrated and included in the election procedures. Significant security concerns relating to the eCMs and the Rally-Tally operations may not be wholly addressable through procedural safeguards, but at the least, a procedural review should address these issues. We recommend that certification review of the systems take into account the documented

---

[182] Page 7 of the State's consultant report (note 73) says, "A feature in Tally that allows administrative users to adjust vote totals for any candidate or issue does not have any data validation or controls to enforce the basic mathematical relationships of the election." The consultants go on to say that the use procedures should recommend restricting administrative access and provide advice on how to reconcile anomalies that might result from using this feature. The *Tally Operations Manual* (note 183) includes only cursory, operational information about security.

[183] *Hart Voting System Tally Operations Manual Revision 43-62B*, Hart InterCivic, Inc., Part No. 6100-049, May 2006, Chapter 4 "Reports", p.118.

procedures for use, and substantive changes to those procedures should trigger some additional review.

We do not believe that the documentation we were provided for our review would be sufficient for state officials to make informed certification decisions. The inadequacy of information provided at the national certification level—the poorly documented testing reports and the complete lack of detailed test plans—combined with the highly referential nature of Hart's documentation put state-level certification at an information disadvantage. The national certification reports largely fail to communicate information one would need to assess the systems with respect to the Voting System Standards. The state consultant reports, while also not providing enough information to replicate their tests, did carefully document serious issues that seem to have slipped through the cracks of the national certification process