Documentation Assessment of the Diebold Voting Systems

Candice Hoke[1] **Dave Kettyle**

Center for Election Integrity
Cleveland State University

July 20, 2007*

This report was prepared by the University of California, Berkeley under contract to the California Secretary of State as part of the "Top-to-Bottom" review of electronic voting systems certified for use in the State of California.

[1] Team Leader. Author affiliation is for identification only.

* Minor typographical and clarification changes were made after July 20, 2007, which are reflected in this document. One footnote was added and two were deleted.

Executive Summary

The California Secretary of State commissioned a comprehensive, independent evaluation of the electronic voting systems certified for use within the State. This team, working as part of the "Top to Bottom" Review ("TTBR"), evaluated the documentation supplied by Diebold Election System, Inc. Our analysis reached a number of conclusions, including:

- *Usability.* When the vendor's documentation is evaluated for its overall usability for local election officials' tasks, its deficiencies significantly outweigh its successes. While some topics and components are well-addressed, conscientious local election officials attempting to master the Diebold system will find the documentation presents numerous impediments to their managing the voting system correctly, in a manner that achieves high accuracy, security, and other core objectives.

- *Federal Testing Labs' Recommendation as Qualified.* The two testing laboratories that were contracted to evaluate the Diebold voting systems produced reports that differed greatly in their thoroughness, degree of detail, and in the adequacy of the bases for their qualification recommendations.

- *Wyle Report: Hardware and Firmware Review.* The reports submitted by Wyle Labs are reasonably thorough, providing details of examinations and testing that were conducted. The reports also analyze the test results, and evaluate these results in light of the federal 2002 voting system standards. The testing also appears to have followed standard methodologies for environmental and electrical testing of electronic components and supporting equipment,

- *CIBER Report: Software and Required Documentation.* The CIBER report on its evaluation of software and documentation pursuant to the 2002 federal standards is unusually brief (16 pages) given the complexity of the required evaluations. None of CIBER's reports on this system discuss in sufficient detail the methodologies, tests, or results that were obtained, and thus do not permit a reader to formulate an informed opinion on the degree to which the Diebold voting system met or exceeded the minimum federal standards for qualification.

- *Security Policy Differences.* Pursuant to the federal standards, Diebold submitted to CIBER a set of voting system security policies that it would mandate for localities purchasing the Diebold system. A comparative analysis shows that the security policies Diebold filed with CIBER were considerably more stringent and extensive than those it ultimately documented in Diebold's product manuals. These sharp differences raise the question of whether California counties are provided with adequate information to implement the security conditions under which the Diebold system was tested and approved.

- *Configuration Audit.* An audit comparing the California-certified configuration of the Diebold voting system with the configured system the vendor provided for the TTBR disclosed numerous differences. A number of these configuration discrepancies involve an uncertified component, and unapproved and largely disabled security settings, raising serious questions about the voting system's accuracy, security, and reliability.

- *Security:* The vendor documentation misses opportunities to assist election officials who are striving to achieve secure elections. The vendor recommends certain security-oriented practices without an explanation of possible vulnerabilities. This approach tends to minimize serious security risks and sidestep mitigation strategies.

Table of Contents

Introduction

The California Secretary of State commissioned a comprehensive, independent evaluation of the electronic voting systems in use within the State. The project, also known as the “Top to Bottom” Review (“TTBR”), involved assigning four teams to each system with each focusing on a different aspect of the voting system. These included teams for source code review, accessibility, and security penetration (also known as the “Red Team”) and documentation review. The teams worked under the overall supervision of the University of California. The Principal Investigators for the project, Professors Matthew Bishop and David A. Wagner, specialize in computer security. This document is the final report of the team that examined the Diebold voting system documentation the vendor submitted to support the system’s certification reviews and ultimately, local election operations using the equipment.

The Diebold documentation review team was located at Cleveland State University and consisted of the two authors of this report plus an additional researcher.[2] We consulted often with the Source Code Review team located at Princeton University,[3] and the “Red Team,”[4] located at the University of California, Davis, and valued greatly these communications. This Diebold Document Review report should be read as a complement to the other two reports filed by the Diebold Source Code and Red Teams, but all of the conclusions offered in this report are solely those of its authors. The work started on May 31, 2007 and ended on July 20, 2007 with the delivery of this report.

Our report assesses the documentation for Diebold Election System, Inc.’s (Diebold) voting system (VS) approved for use in California counties. Materials the Secretary of State (“SOS”) requested for this review included the confidential Technical Data Packages submitted to the Independent Testing Authorities (ITAs) for their qualification testing of the Diebold systems, the evaluative reports produced by the ITAs, and the documentation that is supplied to election jurisdictions in California who purchase Diebold systems. In reviewing the system, the Documentation Teams’ assigned scope included the charge of assessing whether the federal testing laboratory reports supplied adequate documentation for

[2] The Diebold Documentation Review team’s expertise includes technical areas (software engineering) plus analytic assessments of documents and legal standards. Election law professor Candice Hoke (J.D., Yale Law School; Director, Center for Election Integrity; Project Director for the Public Monitor of Cuyahoga Election Reform; Associate Professor of Law, Cleveland State University) served as team leader. David N. Kettyle and Thomas P. Ryan, both of whom served as technical-legal staff for the Public Monitor of Cuyahoga Election Reform, were the other two team members.

As Chapter 3 discusses, the Diebold Documentation Review team did not receive any of the vendor’s technical documentation that it submitted as part of federal qualification testing until July 13, 2007. We chose to use the time between that date and the day this report was due (July 20th) to analyze and report on the almost 1000-pages of documentation rather allocate the scarce time remaining to including extensive citation to legal and other materials. For this background material citation, please consult the reports filed by the other two Documentation Teams (on Hart InterCivic and Sequoia voting systems.)

[3] The Diebold Source Code Team was comprised of David A. Wagner, (team leader), Joseph A. Calandrino, Ariel J. Feldman, J. Alex Halderman, Harlan Yu, William Zeller.

[4] The Diebold Red Team members were: Robert P. Abbott (team leader), Mark Davis, Joseph Edmonds, Luke Florer, Elliot Proebstel, Brian Porter, Sujeet Shenoi, and Jacob Stauffer.

their findings regarding the reviewed Voting System's adequacy under the voluntary federal standards.

Further, the SOS tasked independent documentation review teams to answer two additional major questions about the vendor's documentation taken as a whole. First, is the documentation ***complete***? This question directed us to determine whether the review team had received all the documents that the vendor would have supplied within the certification review process at the federal and State levels. Second, when considering the intended uses of the documentation by county, is the documentation ***sufficient***? Here, we considered whether, when consulted, it adequately supports the county Registrar of Voters' deployment of the VS in a manner that empowers the election officials to administer elections accurately, reliably, and with appropriate security and ballot privacy throughout the election processes. Adequate documentation will assist officials in avoiding errors that can cause systemic problems and alert them to strategies they can employ to prevent (or uncover) malicious tampering with the election equipment or vote totals.

1.1 Scope and Methodology

A voting system's documentation, like that of other technical systems, is normally intended to provide guidance for conducting normal operations and for diagnosing and correcting problems when unexpected situations occur. Where a complex system is at issue, such as the election management and voting device systems that are evaluated in this TTBR project, documentation usability by the intended audiences (for instance, election officials and poll workers) is especially important.

The SOS delineated the basic scope of this review in the Statement of Work (May 2007), with a functional orientation underlying the charge. The three Documentation Review teams (for the three voting systems under evaluation; Hart Intercivic and Sequoia are the other two vendors) then developed some initial methodological principles to guide our assessments and modified our template as needed throughout the review process.

An early focus was the 2002 Federal Election Commission Voluntary Voting System standards (hereafter *VSS*),[5] as it contains some criteria for assessing documentation. We distilled some analytic criteria from the VSS. Because of prior public assignments in Ohio, this Diebold Documentation Review team were able to draw on their prior reports and discussions with Ohio election officials who have been using largely the same Diebold voting system as was the subject of this California review. Our knowledge of some complex tasks that face local election officials, and of unexpected conditions that can arise and for which they need documentation assistance, led this Team to approach a great deal of the review tasks with a pragmatic approach. We began and ended this review motivated by the concern that the documentation provide a high quality of support for conscientious local officials as they go about their important duties.

Our team's work on the VSS analysis and documentation methodology, as well as on TTBR security policies and practices (instituting required physical and electronic security) began in May 2007 after the contracting had largely been completed. Our documentation review officially began in the first week of June, with all analysis scheduled to be completed except for drafting of this report by July 13th. But two of the long-sought Technical Data Packages (TDP) arrived on exactly July 13, 2007— well over one month after they should have been provided and on the exact date that the work scope agreement had stated evaluation work would end. Despite the late date, this Documentation Team proceeded to analyze the TDP documents relating to the most crucial aspects of the federal ITA qualification reviews as well as those that focused on issues that had arisen during the course of this study.

After the documentation arrived, our first task was to conduct an inventory to evaluate its ***completeness.*** As this report establishes, completeness was never achieved despite significant efforts.

[5] http://www.eac.gov/election_resources/vss.html.

We used the ITA citation lists to determine that we had not been provided with any proper "TDP" documentation despite having received a CD that was marked "Diebold TDP." Most of our evaluation period was devoted to the operators' manuals, also known as user manuals, and the ITA reports.

On July 4th, the Diebold documentation team traveled to Sacramento to work in the secure "red team" testing room located in the SOS facility in Sacramento. This trip was designed to permit us to work with the Diebold VS in conjunction with the documentation. While we were not able to conduct a "walk-through" of an entire election preparation and tabulation using the manuals because of certain limitations, we were able to complete some practical tests of the documentation's adequacy. Additionally, we conducted a configuration audit while there. One of the most valuable aspects of the visit was that all team members present were able to discuss the TTBR project and preliminary findings. We also had an opportunity to meet with several California county election officials who visited the red team's testing room.

Throughout the review process, the Diebold Documentation Team provided support and consulted extensively with the other Diebold teams (Red/Penetration Team and Source Code Team) and with the other two voting systems' Documentation Teams.

Partly because of the paucity of technical documentation initially provided, this team's early focus was on the ***sufficiency*** of the documentation. We evaluated its sufficiency in two major respects: (1) whether the documentation supported the ***certification decisions*** that were made approving the system with regard to its accuracy, security, reliability and other criteria; and (2) whether the documentation array designed for counties purchasing the VS was organized and written in a manner that enabled ***local officials to manage and operate the voting system effectively***. The Secretary of State's charge to Documentation Review teams (exclusive of the accessibility team) resulted in our evaluating the documentation's usability and sufficiency for local operations according to core criteria or interrelated axes that included: (a) accuracy and reliability, (b) security; (c) ballot secrecy; (d) auditability, and (e) overall usability for the intended audiences. In general, we considered the local support documentation package as a whole instead of segregating particular manuals for evaluation.

1.2 Limitations

While the incompleteness of the documentation submitted for our review, and the extraordinary tardiness with which the Technical Data Packages were eventually produced, were significant impediments, some limitations of this study can be traced to its being the first of its kind, there being no methodological precedent to follow or improve upon. Future VS assessments will likely not experience the same limitations.

The major limitations on all three documentation review teams included:

- the lack of an opportunity to discuss with local election officials their experiences, and those of the voters in their counties, in using the VS under review;
- the unavailability of operational logs from the voting system that would enable an evaluation of normal and exceptional conditions, including tampering or system failures;
- the fact that the VS components were not observed in use by election staff and voters, in actual election preparation activities, and in voting, tabulation and reporting thereafter;
- time constraints that limited discussion and critique of other teams' reports, both within the Diebold teams and among all Documentation Review team members before the submission date;

- the inability to verify that the operational documentation that was provided to the review teams was the same that was provided to (1) the ITAs and state certification authorities, and (2) the California county election officials; and
- the unavailability of any incident reports and operational questions that have been submitted to the vendors by county election officials, and the responses of vendor personnel.

CHAPTER 2

System Overview

Note: The following overview of the Diebold voting systems that were reviewed for this report is geared toward the non-technical reader who is unfamiliar with election technology. As such, in places it sacrifices technical precision for general accessibility. Readers more familiar with the sorts of technical matters discussed in this report may wish to skip this chapter.

2.1 Voting System Components and Configuration

The Diebold voting system approved for use in California has a central "nerve center" software application named GEMS plus several types of voting devices that can be used by voters to cast ballots. Polling location voting device options include a (1) touchscreen unit named the TSx (usually deployed at Election Day polling locations or for early voting) and (2) optical scanners that read paper ballots, and (3) may be set up to have both voting device options. The TSx is required to include the printer for a paper audit trail so that voters can review and verify their ballot selections before casting their votes. The Diebold optical scan options are subdivided into (a) a "precinct count" system where voters can feed their paper ballot into the scanner that reads and tabulates their votes, and (b) a "central count" system set up to count hundreds or thousands of ballots at the county's offices. The "central count" scanners are linked together using a network that connects to the "GEMS server" – a computer on which the nerve center software is housed. GEMS tabulates the votes from both the touchscreen units and paper optically scanned ballots, and issues reports of voting results.

This section first provides the list of Diebold voting system components approved for California and then discusses them in greater technical and operational detail. California counties determined which of the certified system components would be purchased and deployed within their boundaries, given their resources and other factors.

The SOS provided to the TTBR researchers this listing of certified Diebold voting system components:

- GEMS, v.1.18.24
- AccuVote-TSX with AccuView Printer Module and Ballot Station f/w, v.4.6.4
- AccuVote-OS (Model D) with f/w v.1.96.6
- AccuVote-OS Central Count with f/w v.2.0.12
- AccuFeed
- Vote Card Encoder, v.1.3.2
- Key Card Tool Software, v.4.6.1
- VCProgrammer Software, v. 4.6.1

The "version number" follows the name of each component and designates the particular software program or hardware component that has been approved for use. A component with the same name but a different version number is not legally certified or approved for use within the State. Similarly, any other software program or hardware component that interacts with these certified components is arguably prohibited from use in California unless it receives certification.

Importantly, under the federal Voting Systems Standards of 2002 (hereafter VSS), voting systems are tested, qualified and certified as *systems*, not merely as isolated components. This point is important because a deficiency or incompatibility in one part of a voting system can jeopardize the reliability, accuracy and security of other parts. Thus, when any component is revised or upgraded, with regard to its software (including embedded "firmware") or hardware, the VSS requires that the entire VS within which the component will, or could optionally function, be retested and re-certified. This approach ensures that the upgrade will not trigger unexpected but injurious interference with another portion of the VS.

2.2 GEMS Election Management Software

The GEMS software application is the "election management system" component. It is used in election preparation to create and configure ballots (both electronic and paper ballots), and programs memory cards for use in Diebold voting devices. Post-election, the main GEMS computer or "server" receives voting data from memory cards, tabulates, and then reports election results. GEMS sends or "uploads" configuration data for the AV-OS and AV-TSx units onto memory cards, which then store voting data from ballots cast in the election. These memory cards are then returned to the election offices for vote tallying after the polls close.

At the close of the election and after the memory cards are returned to the county offices, the voting data must be uploaded from the memory cards into the GEMS system for tabulation. This uploading typically occurs via networked devices of the type in which the voting data was stored. The TSx touchscreen memory cards are read by TSx devices linked to the GEMS PC by Ethernet. The memory cards from precinct-based optical scanners (AV-OS) must be inserted into the same type of scanner that recorded the voting data but this scanning unit is connected to the GEMS server. GEMS then deposits the vote data into its election database that was configured by county election employees prior to Election Day.

2.3 TSx Touchscreen Voting Device, VVPAT Printer, and Related Equipment

The Diebold Accuvote TSx is a touchscreen Direct Recording Electronic (DRE) voting machine that according to California law, is required to be equipped with a voter verified paper audit trail unit – otherwise known as a ***VVPAT printer***. The printer is designed to print a record of the voter's ballot choices, which then rolls up into a locked canister inside the TSx unit. The voter does not receive the paper record or a receipt of voting choices registered on the electronic unit but can view and verify the printed choices by looking through a small plastic window after each subset of ballot choices are printed.

The TSx unit is normally deployed to polling places. Its use requires a ***"smartcard***" or "voter access card" to initiate a ballot and authorize the TSx to record votes. A computer chip is embedded in the card. The ***Vote Card Encoder*** is a small hand-held unit slightly bigger than a credit card. Poll workers must be trained to use the encoder so that it will encode the smartcard to bring up the correct ballot (or accessibility functions and options, such as an audio ballot) when the voter inserts the smartcard into the TSx. An activated smartcard permits only one ballot to be cast. After a cast ballot has been recorded, the TSx deactivates the smartcard/voter access card so that it cannot be used to cast a second ballot. The card then emerges, making a clicking sound when it automatically pops partially out from its slot. The voter is to return the smartcard to poll workers, who can then encode it so that it will be usable for subsequent voters.

When the voter (or poll worker) inserts a properly encoded smart card into the TSx, the TSX shows a touchscreen display or activates an audio ballot. As each ballot is cast, the AV-TSX stores an electronic record of the votes associated with that ballot onto a file on the memory card. When the polls have closed, the TSx counts all of the votes and can be directed to print out either a summary tape showing the combined vote tallies without breaking them down by precinct, or a longer tape that shows the tallies by precinct.

Before Election Day, the TSx units require substantial preparation. The GEMS computer is used to generate certain "ballot definitions" that are stored on the memory cards that will be in the TSx units. The ballot definitions store the races, candidate names, ballot issues, and other information in a legally regulated manner. The memory cards are created ("burned") in a process that has some TSx units in the county election offices linked to the GEMS computer; the memory cards receive the ballot definitions via the TSx.

The election officials are supposed to set up logic and accuracy testing for each TSx unit to ensure that when the memory card is inserted, the ballots can be brought up to the screen and will correctly register votes when the on-screen buttons are pushed. Then the memory cards are to be packed into sealed bags and marked for the correct polling place that will use the particular ballots that have been stored on the card, or are left in the TSx units and sealed for delivery to polling places.

The TSx machines are delivered to the polling location with the correct memory card already inserted and inside the locked compartment. Poll workers are instructed to run a ***"zero report***" to demonstrate that the ballot counters are registering zeros—indicating that no votes have been stored n the cards or machine. Poll workers typically are also charged with changing the printer paper as needed in the "AccuView Printer Module."

The TSx runs a Diebold-prepared version of the Microsoft Windows CE operating system. ***BallotStation*** is an additional application loaded on the firmware that provides the user interface that voters and poll workers see on the screen. BallotStation handles a number of crucial functions including managing the interaction with the voter, and accepting, recording, and counting votes.

The TSx memory cards must reach a location that permits voting data to be transferred ("uploaded") into the GEMS computer. Several different options are used in California. Sometimes poll workers are trained to remove the memory card from the machine's sealed slot and pack it for transport to county election headquarters (or to a regional transmission center) so that the electronic vote records can be transferred into the GEMS computer ("uploaded") for tabulation and election results reports. Alternatively, the county can specify that the TSx units are to be transported back to the county election offices with the memory cards undisturbed-- still sealed inside the TSx units. Then the election staff can record and break the seals, and remove the memory cards for uploading into GEMS.

Alternatively, a county might use the TSx internal modem to send vote data to GEMS over the regular phone lines. The TSx can be configured with the telephone number, username and password to connect to the GEMS server. In contrast to the AV-OS, the TSx software uses encryption and authentication software for such calls.

2.4 Optical Scanning at the Polling Place: Precinct Count AV-OS

One version of the Diebold optical scanner, the Accuvote OS (AV-OS), is a "precinct-count" optical scan machine. It is used to scan paper ballots at the polling place. Normally the voter will bring over the paper ballot that has been marked by filling in ovals beside ballot choices. Then, with the poll worker's assistance, the voter feeds the ballot into the scanner for reading and recording the votes. Thereafter, the scanner drops the scanned paper ballot into one of the compartments beneath the scanner, into a locked and sealed ballot box.

During an election, poll workers provide a paper ballot to a valid voter, who then marks the ovals with an approved pen or pencil., When the voter feeds the marked ballot into the AV-OS, the unit scans the ballot, interprets the marked votes, maintains a race counter to increase the vote counts as ballots are read, and then drops the ballot into the locked ballot box. If a voter filled in more than the allowed number of ovals in a given race or question, thus causing an "overvote," the AV-OS can return the ballot to the voter. The voter can then request a new ballot.

The approved California AV-OS "Model D" uses embedded software ("firmware") that is numbered as version 1.96.6. As with the TSx, the precinct count AV-OS memory card must be configured prior to the election with electronic ballot definitions that are created on the GEMS computer. Then, after testing it for accuracy and functionality, the memory card can be left in the slot on the front of the machine or can be packaged and delivered to the polling place for insertion on Election Day. The memory card ballot definition stores the names of races and candidates, plus the directions used for tallying and printing election results reports.

The county has several options for receiving the AV-OS voting data at the close of the election. At the close of the polling place, the unit can be returned to election headquarters with the memory card sealed inside or poll workers can remove the memory card and send it to be uploaded into the GEMS server. GEMS can then tabulate the results and issue the election reports. Or, the internal modem that is embedded in the AV-OS may be used to transmit vote data over the phone lines. If the modem option is used, the AV-OS apparently sends the vote data in the clear with no authentication or encryption.

2.5 Election Office Optical Scanning: Central Count Tabulation (AV-OS)

The AccuVote-OS (also known as the AV-OS) is the same hardware scanner that is used for the precinct count optical scanning but it has a different embedded software ("firmware") installed. Its configuration allows it to be linked with a number of other AV-OS units via a network whereby voting data can be sent into the GEMS server from many scanners concurrently scanning ballot batches. Firmware version 2.0.12 designates the machine is configured for 'central count" as opposed to "precinct count." Central count AV-OS is often used to count absentee ballots as well as provisional and damaged but "remade" paper ballots at county election headquarters or another centralized location.

Unlike the precinct count AV-OS, the AV-OS central count units' operation is largely controlled by GEMS. While the units scan ballots and interpret the ballot marks, the AV-OS central count uploads the voting data to GEMS and does not tabulate or keep any record of votes on the unit. The central count AV-OS memory card needs no ballot definitions and only has some technical information regarding the particular scanner so that it can be individually tracked as it scans ballots. It can be used with or without an automatic ballot feeder called the ***AccuFeed.***

2.6 Additional Certified Software Components

The ***Key Card Tool Software***, v.4.6.1, is used to set security keys for smartcards (voter access cards) and supervisor cards. It can also be used to set passwords for use with supervisor cards. It permits election officials to use a unique security key for each election to make it more difficult to tamper with election equipment by means of unauthorized access cards. A PC-based application, it can be installed on the GEMS computer.

The ***VCProgrammer Software***, v.4.6.1, can be used to program voter access cards to activate the proper ballot on TSx for a given voter. It differs from Voter Card Encoder, which is limited to programming up to 8 different ballots. VCProgrammer can retain and program an unlimited number of ballot definitions for an election, which makes it a better choice for creating voter access cards at early voting locations.

CHAPTER 3

Degree to Which Documentation Was Complete

3.1 Overview

The California Secretary of State specified the range of documentation the voting system (VS) vendors were to provide for the TTBR. The review was to encompass all Diebold technical documentation submitted as a part of the federal testing lab's evaluation as well as all VS operating manuals, among other items. This documentation was to include all manuals that guide the vendor's technicians in initial set up or other work as well as those that support local election officials in their operation of the systems.

The Diebold documentation review team never received all of the expected TTBR documentation, despite this team's follow-up with detailed lists of omissions. A significant part of the technical documentation comprising this vendor's TDP that is mandated by the federal VS standards was never submitted to the Documentation Review team and could not form a part of this review. No TDP documents were supplied to this review team until July 13th, very close to the end of our review.

3.2 ITA Testing Laboratory Documentation

At the outset of this review, we received qualification reports from two Independent Testing Authorities (ITAs) that Diebold had contracted with for the VS evaluations required for qualification under the 2002 federal standards.

3.3 Internal Vendor Manuals

We received a manual designed to guide installation and configuration of GEMS that was specifically restricted to Diebold technical personnel. This was named the GEMS 1.18 Server Administration Guide, Rev. 3.0 numbering 156 pages. No other Diebold documentation of pre-deployment configuration steps was provided.

3.4 Operating Manuals for Local Election Officials

We received the following Diebold operating manuals designed for voting systems customers:

GEMS

- GEMS 1.18 Election Administrator's Guide, Rev. 7.0, 536 Pages. (D0062)

- GEMS 1.18 Election Administrator’s Guide, Rev. 8.0, 543 Pages. (D0087)
- GEMS 1.18 Product Overview Guide, Rev. 2.0, 13 Pages. (D0088)
- GEMS 1.18 Reference Guide, Rev. 6.0, 365 Pages. (D0063)
- GEMS 1.18 Reference Guide, Rev. 7.0, 351 Pages. (D0080)
- GEMS 1.18 Reference Guide, Rev. 8.0, 355 Pages. (D0089)
- GEMS 1.18 System Administrator’s Guide, Rev 5.0, 97 Pages. (D0064)
- GEMS 1.18 System Administrator’s Guide, Rev 6.0, 95 Pages. (D0090)
- GEMS 1.18 User’s Guide, Rev. 12.0, 281 Pages. (D0086)
- GEMS 1.18 User’s Guide. Rev 11.0, 280 Pages. (D0065)
- JResult Client 1.1 User’s Guide, Rev. 1.0, 28 Pages. (D0091)

Optical Scanning – General Resources

- Ballot Specifications, Rev. 2.0, 18 Pages. (D0056)
- AccuVote-OS Hardware Guide, 124 Pages. (D0055)
- AccuVote-OS Hardware Guide, Rev 4.0, 102 Pages. (D0059)
- AccuVote-OS Hardware Guide, Rev. 5, 97 Pages. (D0066)

AV-OS Central Count

- AccuFeed 1.0 Hardware Guide, 40 Pages. (D0053)
- AccuFeed User’s Guide, Rev. 1.0, 7 Pages. (D0054)
- AccuVote-OS 2.0 Central Count User’s Guide, Rev. 3.0, 80 Pages. (D0058)
- AccuVote-OS Central Count 2.00 User’s Guide, Rev. 4.0, 85 Pages. (D0060)
- AccuVote to Digi PortServer II (PSII), 2 Pages. (D0061)

AV-OS Precinct Count

- AccuVote-OS Pollworker’s Guide, Rev. 2.0, 105 Pages. (D0067)
- AccuVote-OS Pollworker’s Guide, Rev. 3.0, 116 Pages. (D0068)
- AccuVote-OS Precinct Count 1.96 User’s Guide, Rev. 4.0, 209 Pages. (D0069)

TSx and Related Equipment

- AccuView Printer Module Hardware Guide, Rev. 1.0, 29 Pages. (D0077)
- AccuView Printer Module Service Guide, Rev. 1.0, 13 Pages. (D0076)
- AccuVote-TSX Hardware Guide, Rev. 8.0, 177 Pages. (D0072)
- AccuVote-TSX Pollworker’s Guide, Rev. 5, 117 Pages. (D0073)
- Ballot Station 4.6 User’s Guide, Rev. 1.0, 149 Pages. (D0078)
- Key Card Tool 4.6 User’s Guide, Rev. 1.0, 20 Pages. (D0092)
- Upgrading Voter Card Encoder Firmware, Rev. 1.1, 4 Pages. (D0093)
- VCProgrammer 4.6 User’s Guide, Rev. 1.0, 29 Pages. (D0095)
- Voter Card Encoder 1.3 User’s Guide, Rev. 1.0, 30 Pages. (D0094)

CHAPTER 4

Adequacy of Support for Qualification Recommendations

4.1 ITA Qualification Testing Laboratory Reports

The federal standards under which the Diebold voting systems were evaluated accord a pivotal role to Independent Testing Authorities' (ITA) evaluations. At the time that the Diebold systems under review here received California certification (February 17, 2006), the ITA laboratory reports formed the primary basis for the "qualification" determinations made by the National Association of State Election Directors (NASED).[6] The Diebold system was reviewed and qualified by NASED under the technical standards found in the 2002 Voting System Standards (VSS)[7] and not the newer 2005 VSSG. The 2002 VSS is comprised of two volumes which specify performance standards and also the testing and examinations required for VS qualification.

At the time the Diebold systems were reviewed for federal qualification, the ITAs exercised an almost unique role and set of powers over voting systems used in this country. Given that the VS vendors have typically asserted proprietary rights and access restrictions over the source code, documentation resources, and election databases, and because State governments have generally deferred to the ITA examination regime, virtually no entities and examiners other than the ITAs have had the opportunity to evaluate the accuracy, security, and other attributes of the voting systems either for compliance with the governing standards or according to independent criteria. The ITA report is expected to reveal in extensive detail the integral parts, component operations, the scope of testing with all test results, and overall systemic functioning of the VS submitted for review. To complete these extensive evaluations, under the 2002 VSS vendors were required to submit their voting system source code, documentation, and hardware to the ITA.

[6] NASED no longer has the role and powers that it did at the time this Diebold system was qualified. Currently, as a result of federal regulatory changes, the U.S. Election Assistance Commission (EAC) has assumed the former powers to receive the independent laboratory reports and determine satisfaction of the federal VS criteria. This new EAC "qualification" will essentially mean national certification.

Independent testing lab supervision has been reallocated as well as. NIST now has the power to recommend accreditation for test labs to the EAC, rather than NASED. A name change has also occurred with the new certification regime: accredited test labs are now known as voting system test labs (VSTLS) rather than ITAs. Because the Diebold system received qualification under the former regulatory structure, this Report refer to the test lab reports as issuing from ITAs.

[7] The 2002 VSS have been heavily criticized for various deficiencies, including lack of technical precision and the omission of their being mandatory minimum standards for all voting systems used in any of the nation's elections. Later this year, on December 31, 2007, the 2005 Voluntary Voting System Guidelines will become the guidelines for federal certification and "[a]l previous versions of national standards will become obsolete." U.S. Election Assistance Commission, Voluntary Voting System Guidelines, http://www.eac.gov/vvsg_intro.htm (visited July 18, 2007).

As authorized, Diebold contracted with two ITAs to conduct the required VS evaluative tests: Wyle Labs and CIBER, Inc. These tests were divided into hardware and software plus documentation review. Wyle conducted the hardware and firmware reviews for the AccuVote-OS and AccuVote-TS, and CIBER reviewed the GEMS software and related software components. In addition to testing hardware, a hardware ITA tests “firmware” – the software that is embedded in voting system equipment. The software ITA normally evaluates all other software used in the system. It conducts a source code review as well as other tests. In fulfilling the federal VSS charge, the ITA completes three types of testing on the submitted voting system: functional testing, environmental testing, and the source code review.

To be a complete under the 2002 VSS, the ITA report on a component or system should include:

- ***Test Plans***: a presentation of the test plans, descriptions of the tests conducted, and the reasoning that the ITA applied to reach each of its conclusions regarding satisfaction of a particular standard or test;

- ***Matrix:*** a requirements matrix derived from the 2002 VSS; for each requirement in the matrix, the ITA notes whether the application was tested and, if so, whether the system met the requirement;

- ***Technical Documentation:*** the specified contents of the technical data package (TDP) must be submitted to the ITA; in addition to the ITA’s statement that it has reviewed the TDP contents, the ITA report should demonstrate the criteria applied to determine the TDP contents’ adequacy under the 2002 VSS;

- ***Longitudinal Testing Documentation:*** a review of the scope of testing and retesting that occurred over time; it is expected that an ITA report on a VS will show many instances of revision and ITA retesting; because every upgrade and version revision requires additional VS qualification, a VS normally has a substantial testing paths that can (and should be) be tracked in the report.

The SOS asked TTBR document review teams to determine whether the reports these ITAs filed are "sufficient," meaning that the reports document the tests conducted and report the results that the VS earned in the evaluations, yielding a reasonable confidence that the evaluations were conducted according to the 2002 testing standards. To this end, we examined the two labs’ testing methodologies and their presentation of test data but we did not attempt to reproduce the testing, reinterpret the test data, or reconsider the ITAs’ recommendation that the VS receive federal qualification. We also did not consider whether we might have conducted the testing differently.

The two ITAs pursued two quite different approaches to testing and reporting which cannot be explained simply on the basis of their different testing duties.

Table 4.0 Diebold VS Component Qualification Testing Allocation

CIBER, Inc.	***Wyle Laboratories, Inc.***
GEMS 1-18-24	AccuVote-OS Model D Precinct Count f/w 1.96.6
GEMS 1-18-24 with BallotStation 4.6.4	AccuVote-TSx with AccuView, f/w 4.6.3
Express Poll 2000/4000	AccuVote-TSx with AccuView, f/w 4.6.2
GEMS 1-18-24	VCProgrammer 4.6.1
	Key Card Tool 4.6.1
	*AccuVote-TSx with BallotStation 4.6.4

4.1.1 Wyle Report

In testing VS hardware and firmware, Wyle was required to evaluate the physical properties of manufactured components and logical correctness of computer code. The Wyle hardware testing appears to have followed standard methodologies for environmental and electrical testing of computer components and supporting electrical components. It seems, quite appropriately, to track some of the testing performed earlier by a laboratory on Diebold's behalf during product development. Wyle's report describes its methodology and other aspects of the test plans in substantial detail. It presents and analyzes the resulting test data as a basis for Wyle's recommendation to NASED that the VS be qualified under the 2002 VSS.

The Wyle report[8] adequately tracked the version numbers of the components under review. In evaluating the source code for the firmware under review, Wyle seems to have relied extensively on automated tools for finding deviations from coding standards or uses of prohibited flow-of-control constructs. Perhaps for this reason, the results of its source code examination seem to emphasize form.[9]

It appears that Wyle properly noted and tracked the version designations of specific Diebold election products as it tested and reported on the performance of Diebold products.

Wyle did note that it had not tested certain aspects of the AccuVote-TSx and AccuVote-OS. Its ITA report indicates the VS was not tested, on the following points:

- 2.2.5.2.3 Test for the capability for a jurisdiction to designate critical status messages
- 2.2.8.2(m) Support of cumulative voting.
- 2.2.8.2(n) Support of ranked over voting.
- 2.2.10 Telecommunications (Hardware Functional & Software System Level Test.)
- 3.2.8.2 Generation of output reports at the device, polling place and summary levels, with provisions of administrative and judicial subdivisions as requirement (sic) by the jurisdiction.
- 3.4.5(c) DRE and paper-based precinct count systems and supporting software respond to operational commands and accomplish the functions of consolidation of vote selection data from multiple precinct-based systems, generate jurisdiction-wide vote counts, store and report the consolidated vote data.
- 3.4.5(c) DRE and paper-based central count systems and supporting software respond to operational commands and accomplish the functions of consolidation of vote selection data from multiple counting devices generate jurisdiction-wide vote counts, store and report the consolidated vote data.
- 4.3(a) and (b) During an election, the integrity of vote and audit data is maintained and protected against any attempt at improper data entry or retrieval.

On the basis of the materials we received it appears the Wyle Lab conducted a broad range of tests and engaged in detailed analytic reporting on the adequacy of the test results. In our view, taken as a whole the Wyle reports provide substantial evidence in support of its recommendation that the Diebold VS receive federal qualification under the 2002 VSS.

[8] *Hardware Qualification Testing of the Diebold Election Systems AccuVote Optical Scan Model D Precinct Ballot Counter (Firmware Release 1.96.6).*

[9] While some coding standards aid readability, maintainability and security, and may reduce the likelihood of several classes of bugs, automated code analysis has some notable deficiencies and cannot suffice for comprehensive code assessment.

4.1.2 CIBER Report

In contrast to the test reports from Wyle, the CIBER Qualification Test Report (D0044) issued for GEMS 1.18.24 is brief and perfunctory. It fails to include basic information that is essential to establishing the functionality, reliability, security and certification status of GEMS itself, or of proposed or anticipated GEMS configurations. The report's 16 pages are devoted primarily to broad generalizations drawn from the 2002 VSS and do not sufficiently elaborate on any specifics of the testing methodology, test results or bases for its recommendation that GEMS 1.18.24 be qualified.

The report's cursory recitals fail to offer any basis for assessing the adequacy and repeatability of any testing or analysis that CIBER may have performed on the software. At no point does it demonstrate that an adequate evaluative review of GEMS and its associated systems was undertaken. The CIBER report does not describe the VSS-required vendor submission of various test plans, nor does it discuss conducting detailed tests or the test results that were thereby obtained. In scope, substance, and style, the CIBER report on the GEMS software resembles Wyle's Executive Summary of its qualification report for the AccuVote-TSx with AccuView Printer Module.[10]

While the length of CIBER's report alone is not dispositive as to its adequacy, it is interesting to note that a subsequent report issued by CIBER and documenting a highly circumscribed test effort (involving some report scripting code resident in a Diebold voting device), spans 13 pages—which is nearly as long as the entire 16-page GEMS qualification test report. (D0042). Because of their extreme brevity and lack of particulars, the CIBER reports do not permit the documentation review team to discern what kind of testing was completed. The reports simply assert the adequacy of the system and its component parts under review rather than establish a basis for understanding any testing and analysis that was completed.

4.1.3 The Technical Data Package: Selected Analysis

In assessing the vendor documentation and the ITA testing, we were able to review part of the vendor-supplied Technical Data Package (TDP) that the 2002 VSS mandates for submission when the ITA qualification review is initiated. We were accorded access to the TDPs for GEMS and for the AccuVote-TSx. The vendor did not submit to the TTBR specialized TDP documentation for the optical scanning systems or for any software other than GEMS.

While the submissions were not structured according to the organization of the TDP definition found in the VSS, each TDP included a "TDP trace" document which was helpful in mapping the documentation provided in the TDP to the subject-specific sections of the TDP format.

Many TDP sections refer to the customer documentation as a source of technical or operational information. In addition to missing TDP materials for several Diebold systems, some of the customer documentation that is incorporated by reference into the technical documents that we reviewed was not submitted for the TTBR. The gaps in vendor documentation relate to many aspects of the Diebold voting systems under review.

Accuvote TSx The TDP for the AccuVote-TSx included extensive information about the design, manufacture, assembly, and testing of these DRE voting machines. The specifications as provided by the component vendors include those for many electrical and electronic components that are integrated into

[10] Compare, *e.g.,* D0100 *Wyle Test Report: Hardware Qualification Testing of the Diebold Election Systems AccuVote-TSx DRE Voting Machine with AccuView Printer Module, p. 5,* Section 1.3 "Summary." The Qualification Test Report (D0044).

AccuVote-TSx. These parts from other vendors are subject to quality and conformance standards for manufactured parts; technical information is supplied documenting the internal controls for hardware development and manufacture. These TDP documents also include descriptions of Diebold's programs for establishing and maintaining relationships with its suppliers and seeking to ensure a reliable stream of quality components.

The TSx technical documentation supplied in the TDP covers the spectrum from the very detailed and concrete, for example. the placement of screw holes for mounting the motherboard of the TSx, to statements that are abstract and aspirational, such as a corporate vision statement comprised of a series of sentences starting with "*We Believe....*" As such, the TDPs provided by Diebold are not so much a set of documents created or adapted to address the VSS requirements for a TDP as they are a large, over-inclusive set of pre-existing documents submitted to cover all the subject areas prescribed for a TDP.

Some details of the Diebold TDP submission bear a further note:

- The portion of the GEMS TDP devoted to what Diebold calls "operating system-level safeguards intended to protect against tampering"[11] is simply an unattributed reproduction of a chapter of the 1995 Microsoft publication entitled *MS Windows NT Workstation 4.0 Resource Guide.*[12] The chapter is called "Windows NT Security,"[13] and discusses the overall security framework of the Windows NT operating system. While informative, the Microsoft guide contains a broad overview of system and network security models, as implemented in Windows NT. It does not indicate which, if any, of the Windows NT security features described in the chapter are employed in securing a GEMS server. The information in the chapter is readily available, public information that has little direct applicability to the election management context. It is the sort of information that a qualified testing organization can be expected to know or be able to locate if needed. Further, any ITA seeking to do a realistic assessment of GEMS would base that assessment on the security features of the actual platform on which the system is being tested (Windows 2000 Server) rather than those of a predecessor platform (Windows NT 4.0).[14]
- The exclusive discussion in the TDP of the platform security specifications of Windows NT 4.0 seems out of place with the repeated assertions in the TDP that GEMS was designed for Windows XP, the fact that the Server Administrator's Guide and other documentation describes installing GEMS on Windows 2000 Server, and the fact that the GEMS server provided to the TTBR study was running Windows 2000 Server. For a discussion of platform configuration issues, see Section 4.3 *Configuration*.
- One troubling finding based on a comparison of the TDP and the customer documentation supplied by Diebold is that the security policy presented in the Diebold customer documentation differed significantly with the mandatory client security policy that Diebold submitted to the ITA. See Section 6.1 for an extensive discussion of this issue.

[11] *GEMS 1.18 Technical Data Package – System Functionality Description*, p. 2-4.

[12] The original Microsoft publication is available at: http://www.microsoft.com/technet/archive/ntwrkstn/reskit/default.mspx, accessed 7/17/2007.

[13] The chapter included in the GEMS TDP is available at: http://www.microsoft.com/technet/archive/ntwrkstn/reskit/security.mspx, accessed 7/17/2007.

[14] Note that the Microsoft publication from which the appendix is copied contains the following notice:

> "© 1995 Microsoft Corporation. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation." No such written permission is included in the GEMS TDP.

4.1.4 Are the ITA Recommendations to NASED Adequately Supported By the Documentation?

The CIBER report does not support a confident conclusion that the testing laboratory evaluated the source code or the technical documentation for its compliance with federal 2002 VSS. The Wyle hardware and firmware report is substantially more extensive than the CIBER report but limitations in the documentation supplied for our review prevent us from fully assessing the adequacy of the Wyle evaluations for supporting NASED qualification.

4.2 State Certification

The central regulatory charge to the Secretary of State incorporates interpretive breadth and the possibility for varying standards over time. The primary statutory charge to the Secretary of State is found in California Election Code § 19205 (emphasis added):

> The Secretary of State shall establish the specifications for and the regulations governing voting machines, voting devices, vote tabulating devices, and any software used for each, including the programs and procedures for vote tabulating and testing. The criteria for establishing the specifications and regulations shall include, but not be limited to, the following:
>
> **(a)** The machine or device and its software shall be *suitable for the purpose* for which it is intended.
>
> **(b)** The system shall *preserve the secrecy of the ballot*.
>
> **(c)** The system shall be *safe from fraud or manipulation*.

Diebold’s voting system has traversed a somewhat rocky California regulatory road which has included certification, decertification, and re-certification. The Certificates that have issued permitting the VS to be used within the State have carried some significant restrictive conditions. The State certification system records provided for this review do not reveal any independent source code testing or repetition of the VSS review at the time the Diebold VS was presented for re-certification, but the records are not extensive or illuminating and a source code or other extensive review might have occurred.

4.2.1 California State Certification Process

The certification testing of Diebold systems conducted by the State of California and its designees was successful in validating crucial aspects of election system performance and uncovering problems that needed to be addressed prior to certification by the Secretary of State. Though the scope of the testing was more circumscribed and the access to some types of vendor information more limited than was the case for ITAs testing the same systems, California's testing was arguably more thorough and helpful in advancing the objectives of accuracy, reliability and security than the testing performed by ITAs.

The reports[15] issued by those entities testing the Diebold systems on behalf of the State were far superior to those issued by CIBER, the ITA hired by Diebold to perform qualification testing of its GEMS product. In contrast to the CIBER reports covering the same systems, the State reports have thorough system configuration information[16] and discussion of test objectives, methodologies, and limitations. Also unlike the CIBER reports, the State reports included detailed information about the nature and frequency of failures and anomalies, and included some primary test data that gave an accessible illustration of the testing procedures.

Perhaps as important as the State testing itself was the apparent success with which the State was able to work with Diebold to make beneficial changes to its products in response to unsatisfactory test performance. This cooperative approach to resolving problems with election technology may help bring about additional changes to Diebold systems to better advance the accuracy, reliability and security of

[15] See *Staff Review and Analysis Report*, Prepared by the Secretary of State Elections Division, November, 14, 2005, and Steven V. Freeman, *Certification Test for the Diebold Election Systems, Inc. (DESI) GEMS 1.18.24, AV-OS 1.96.6, AV-TSX 4.6.4 with AccuView Printer Module, and Voter Access Card utilities*, November 11, 2005.

[16] See Steven V. Freeman, *Certification Test for the Diebold Election Systems, Inc. (DESI) GEMS 1.18.24, AV-OS 1.96.6, AV-TSX 4.6.4 with AccuView Printer Module, and Voter Access Card utilities, Attachment A*, November 11, 2005.

elections in California.

Some room for improvement exists in the formal presentation and transmittal of procedural safeguards intended to address issues uncovered in testing. Future reports might better serve the Secretary of State and election officials by consolidating express recommendations for usage procedures intended to mitigate problems discovered in testing. The reports we examined had mixed together proposed policy statements with the test results and technical findings.

4.3 Configuration Issues: Nonconformity with Certified Configuration

In the VS testing and certification regime, the most extensive testing is reserved for voting system components that are designed by the election system vendor to handle election-related functions. In the case of software components, the testing involves a review of the source code. Some "commercial off the shelf" (COTS) software that is distributed with the VS is subject to less rigorous testing standards, though it must be tested as part of overall system testing.

In evaluating and comparing the vendor documentation, ITA test reports, certification documents and the vendor-configured Diebold VS submitted for the TTBR, we found configuration differences that raise questions about the consistency with which certain voting system components are provided to customers in the configurations for which they were certified. By analyzing the results of a configuration audit we conducted on the Diebold VS submitted for the TTBR, we discovered some significant inconsistencies between parts of the VS that are or were:

- described in the vendor-supplied documentation;
- the subject of a successful qualification or certification review;
- actually being deployed in California counties; and those
- submitted by the vendor for TTBR testing in California.

The table comparing the range of differences follows this section and is identified as ***Table 4.3, Configuration Comparison.***

Some discrepancies are of comparatively little concern. Certain COTS support applications on the GEMS server, for example, have been deployed with minor version variations. While not ideal, these variations do not necessarily have the same significance as other discrepancies discussed below.

Because of the differences in configuration we present below, we are unable to conclude that the vendor submitted to the ITA the requisite documentation germane to the sought VS certification for a particular configuration. Nor can we conclude that the officially qualified and certified VS (whether for federal or State reviews) is the exact VS that is currently being deployed in California counties that use Diebold equipment. Determining which California counties, if any, are currently using the Diebold VS in an uncertified configuration is beyond the scope of this review.

4.3.1 Uncertified Components and Configurations

As discussed below, we find that certain Diebold VS configurations that are widely used in California counties may not have been federally qualified or State certified. For the affected counties, integration of uncertified VS components among certified components may render the voting system as a whole uncertified for use in California.

4.3.1.1 JResult Client

As part of its GEMS product, Diebold's distributes a Java-based application program called JResult Client. JResult Client is used for periodically generating visually-appealing updated reports of election results for public display and for posting on the Web as tabulation proceeds on election night.[17] JResult Client is pre-installed on GEMS servers prior to delivery to customers.[18] It can also be installed and used on Windows-based PCs other than the GEMS server.[19] We believe that the presence of JResult Client on GEMS servers in California raises a number of very serious concerns about the integrity of the GEMS servers deployed in California, as well as their legal status.

As illustrated below, there is no evidence in any documentation we have reviewed that JResult Client has been submitted, with the required documentation and source code, for testing by an ITA. There is no evidence that it has qualified under federal standards, been submitted for certification in California or been certified for use in California. The California certification of GEMS 1.18.24 was granted with the condition that "[n]o additional software developed by the Vendor other than that specifically listed in this certificate shall be installed on a computer running GEMS version 1.18.24."[20] These facts raise substantial doubt as to the certification status of any GEMS server in use in California that includes JResult Client. As such, it is possible that GEMS servers in use throughout California are used in an uncertified configuration.

JResult Client is installed on and can be run on the GEMS server machine, a separate Windows workstation, or both.[21] As its documentation, configuration and persistent interaction with GEMS make clear, JResult Client is a GEMS component and not a COTS item. JResult Client is a Diebold-developed application, written and deployed to facilitate election management activities on the GEMS server. The documentation specifies that a Diebold technician or an election administrator shall install JResult Client as a "component" of the GEMS product via the GEMS install wizard.[22] The JResult Client User's Guide is distributed with the other GEMS documentation.[23] JResult Client cannot function apart from its interaction with the GEMS Results Server. JResult Client is also included as a Diebold product in the Diebold Election Systems' Bugzilla database.[24]

JResult Client does not appear on the list of software submitted for ITA testing[25] or recommended for federal qualification.[26] It does not have a Qualification Number. It was not submitted for California certification, does not appear in the detailed configuration specification included in the California certification testing report,[27] and does not appear on the California certificate.[28] It is installed as part of

[17] *GEMS 1.18 System Administrator's Guide, Revision 5.0,* p. 1-2.

[18] *GEMS 1.18 Server Administrator's Guide, Revision 3.0*, p. 2-51.

[19] *GEMS 1.18 Server Administrator's Guide, Revision 3.0*, p. 1-3.

[20] Secretary Of State of California, *APPROVAL OF USE OF DIEBOLD ELECTION SYSTEMS, INC. DRE & OPTICAL SCAN VOTING SYSTEM,* Section 4(a), February 17, 2006.

[21] "JResult Client may be installed and operated on the GEMS server, in addition to the designated JResult Client machines." *GEMS 1.18 System Administrator's Guide, Revision 5.0,* p. 2-7.

[22] *GEMS 1.18 Server Administrator's Guide, Revision 3.0*, p. 2-51.

[23] *GEMS 1.18 Product Overview Guide, Revision 2.0*, p. 2-2.

[24] *Bugzilla User's Guide, Revision 1.0,* p 9. (This document is a customized guide for use within Diebold Election Systems, Inc.)

[25] *Software Functional Test Report, Diebold Election Systems GEMS 1-18-24, Version 1.0*, CIBER, Inc., August 3, 2005, pp. 2-3.

[26] *Software Functional Test Report, Diebold Election Systems GEMS 1-18-24, Version 1.0*, CIBER, Inc., August 3, 2005, p. 8.

[27] *Staff Review and Analysis Report*, Prepared by the Secretary of State Elections Division, November, 14, 2005,

GEMS and was present, in compiled form, on the GEMS server provided by Diebold to CIBER[29] and the GEMS server provided by Diebold for the TTBR study.[30] This server, Diebold representatives assured us, was configured in the same manner as the other GEMS servers sold to California election jurisdictions.

A directory listing included in *Addendum 5* to the CIBER testing report for GEMS 1.18.22 indicates that the compiled JResult Client application files were present on the GEMS server submitted for ITA testing. This is the only reference to JResult Client contained in the CIBER report. It is not clear why CIBER did not flag this software in its report or seek more information about JResult Client from Diebold prior to recommending qualification of the system. Neither the source code nor the system design for JResult Client appear to have been reviewed by CIBER and were likely not submitted by Diebold for CIBER's review. The CIBER report lists programming languages employed in the source code they reviewed, and Java appears nowhere on this list. The GEMS TDP includes no description of the JResult Client design or testing and includes no coding standards for Java programming.

While the non-certification of JResult Client in California, by itself, compromises the integrity of elections in California jurisdictions using GEMS, we discovered several specific issues with JResult Client that we believe make its presence and use on election equipment in California cause for very serious concern.

The first issue is that the GEMS documentation describes an approved use case in which JResult Client, running on the GEMS server, posts election results to an FTP server connected to the Internet.[31] The establishment of such a link, however indirect, between the GEMS server and the Internet should be thoroughly examined as a matter of election security.

The second issue of great concern is that JResult Client and the GEMS Results Server interact with a common resource on the GEMS machine, or on a networked machine.[32] An examination should be done into potential concurrency problems that could cause the processes to collide and threaten the stability of the GEMS server during election tabulation.

Also of concern is the specific JResult Client configuration as installed on GEMS servers. Both the file listing in the CIBER report addendum mentioned above, and our own configuration audit of the GEMS server provided to the TTBR reveal that the GEMS installation script copies both individual Java class files (bytecode files) and a JAR file containing the class files to the JResult Client installation directory on the GEMS server. This is not only a configuration management problem, but a potential vector for an attack. An attacker with access to the GEMS server could, for example, copy modified class files to the GEMS server in place of the original files. These potentially malicious class files could be executed in place of the code in the JAR file by making a small change to the CLASSPATH environment variable or to a batch file that invokes the JResult Client program. This malicious code may evade detection because anyone verifying the signature on the JAR file would find that it has not been modified and conclude that the JResult Client application in use on the GEMS server has not been modified. The fact that this configuration defect was not noticed or not reported by CIBER is also cause for concern about the thoroughness of their testing of GEMS.

and Steven V. Freeman, *Certification Test for the Diebold Election Systems, Inc. (DESI) GEMS 1.18.24, AV-OS 1.96.6, AV-TSX 4.6.4 with AccuView Printer Module, and Voter Access Card utilities*, November 11, 2005.

[28] Secretary Of State of California, *APPROVAL OF USE OF DIEBOLD ELECTION SYSTEMS, INC. DRE & OPTICAL SCAN VOTING SYSTEM,* Section 1, February 17, 2006.

[29] *Addendum 5* of the to the CIBER testing report for GEMS 1.18.22.

[30] *See* Section 4.3.2 *Configuration Audit, infra*.

[31] *GEMS 1.18 Election Administrator's Guide, Revision 8.0,* p. 16-15.

[32] *GEMS 1.18 Election Administrator's Guide, Revision 8.0,* p. 4-128.

Finally, as best can be determined from the materials provided, the JResult Client program (and its accompanying documentation) were not present on the GEMS server that Diebold submitted for certification testing in California. Given the presence of JResult Client on the GEMS server this team analyzed, and the internal GEMS configuration manual's instructions to Diebold technicians to install JResult Client as part of the standard GEMS installation, the question arises of why the vendor excluded JResult Client from its California certification submission.

4.3.1.2. COTS, Windows OS, and Other Configuration Irregularities

In assessing the VS configurations, we found that Diebold systems were deployed with a range of different COTS software components other than those that were tested and those that appear in Diebold’s internal and customer documentation. There were several, somewhat minor applications that were slightly different from the tested and documented versions (file archive utility, audio recorder and codec).

Some COTS applications were present on the TTBR GEMS server that were not part of any tested and documented configuration. These programs should not be installed on any election server at all (e.g., Outlook Express, NetMeeting).

Windows OS Version Differences More worrisome than the variations in COTS application programs, however, is the fact that the GEMS documentation, testing, certification and deployment documents do not agree on which Windows operating system versions GEMS should or could be installed. As explained above, the TDP section on platform security exclusively discusses Windows NT 4.0.. Elsewhere in the TDP, it notes that GEMS was designed to be run on Windows XP. Yet the GEMS internal and customer documentation describes how to install, configure and maintain GEMS on the Windows 2000 Server and no other system. Finally, the ITA test report indicates that their testing was done using GEMS on Windows 2000, and the GEMS server supplied to the TTB ran Windows 2000.

Unlike small version changes in the minor COTS utility applications described above, differences in an operating platform generate significant implications for reliability and safety that need to be explored and thoroughly tested. Though the Windows operating systems listed are related to one another and share many features and capabilities, GEMS needs to be designed, tested, documented and deployed for a common operating system or systems. Crucial, ongoing configuration and updating tasks essential to securing the GEMS server, for example, are performed differently for different Windows versions, and each one needs to be tested and documented if it is to serve as a platform for the GEMS application. (Though we have no way of knowing the cause of the severe mis-configuration of crucial security settings on deployed GEMS Windows 2000 machines that we outline below, such mis-configuration could be the result of a Diebold installation procedure that does not properly follow the specific steps required to configure certain settings on Windows 2000 machines.)

4.3.2 The Configuration Audit

We performed a configuration audit of the GEMS server supplied for the TTB review (the “TTBR GEMS server”). Diebold technical representatives confirmed that it was assembled by Diebold and that they configured the hardware and software exactly as it would be upon delivery to a California county that was purchasing such equipment. We then compared the configuration of the TTBR GEMS server to the configuration set forth in the *GEMS 1.18 Server Administrator's Guide, Revision 3.0*, and to the configuration of the GEMS server evaluated by CIBER for the August 3, 2005 report recommending GEMS 1.18.24 for NASED qualification.

When compared, the configurations showed many similarities, but some variations were noticeable. At least a few variations may figure in the relative accuracy, reliability and security of the Diebold election system. Additionally, some of these variances appear to deviate from the certified configurations for use in California elections.

The terms of the VSS reflect the accepted fact that components of computer systems cannot be evaluated without reference to the other components with which they must interact. Any faulty or malicious piece of software or hardware in a computer system could compromise the entire system. Furthermore, two separate components in a system may be incompatible, may interfere with one another or may not work well together. Configuration changes may bring to life latent bugs in a system component that were not evident before. In short, configuration management is crucial, and is accorded an entire chapter of the VSS.[33]

The *GEMS Server Administrator's Guide* is a document available to and used by Diebold technical personnel to configure systems prior to releasing them to the election system customers. It walks through step by step procedures for installation of the operating system and software, and covers setting various settings in the operating system, the GEMS application, and other aspects of the software environment. The document clearly states that it is not permitted to circulated beyond vendor personnel, and thus is unavailable to customers. Furthermore, the topics and configuration choices covered in the *Guide* are not explained to the election official customers in the customer documentation. For this reason, correct configuration of the GEMS server by the Diebold staff prior to delivery of the machine is essential; the customer will not have the needed guidance to remedy any mistakes, and may not even detect them..

We found several important areas in which the GEMS configuration settings in the *GEMS Server Administrator's Guide* were not adhered to by Diebold personnel when they set up the TTBR GEMS server. This resulted in significant configuration deviations from the documented specifications. We also found several areas in which the *GEMS Server Administrator's Guide*, even if followed exactly, does not yield an acceptable configuration for use by an election jurisdiction.

Several software packages that were to be installed according to the *GEMS Server Administrator's Guide* were not installed on the TTBR GEMS server. Additionally, as the configuration audit table illustrates, several applications were present on the TTBR GEMS server that were not called for in the *GEMS Server Administrator's Guide* and which are not appropriate for a secure election server.

Perhaps most importantly, we found crucial security settings that were not configured correctly on the TTBR GEMS server. The security policy on the TTBR GEMS server was not set up to log any security events through the Windows event logs. There were no restrictions configured to limit the access by ordinary GEMS users to core operating system functions and settings. No password policies or other security policies were implemented to bring the security of the system up to an acceptable level of confidence in mission critical, sensitive election equipment.

The TTBR GEMS server, as delivered and configured, was not suitable for use by any county without significant reconfiguration. Because these crucial aspects of the configuration of the GEMS server are to be implemented by Diebold personnel and are not described in any customer-accessible manual, an election jurisdiction would have no source of information on how to bring about the proper, certified configuration, and may indeed not be able to recognize that the configuration is not correct.

[33] VSS, Vol. I, section 8; configuration audits are delineated in section 8.7.

Table 4.3 Configuration Comparison

The following table presents the types and versions of various components of the Diebold VS encountered in different documents and deployed systems examined for the TTBR.. The table compares the equipment submitted by Diebold to the TTBR, the systems described in the GEMS Server Administrator's Guide, the systems reviewed during ITA testing, the systems reviewed during certification testing in California, and the systems as ultimately certified for use in California. Individual names and version designations are given with as much specificity are possible, and thus may not be uniform for all entries in a row. See section 6 of this report for information on security-related configuration issues.

	TTBR Equipment Configuration Audit	GEMS Server Administrator's Guide	ITA Reviewed Configuration	NASED Qualified as N-1-06-22-22-002	Cal. Test Configuration Report of 11/11/2005	SoS Certified on 2/17/2006
GEMS Software	1-18-24	Written to encompass several GEMS versions.	1-18-24	1-18-24	1-18-24	1-18-24
AVOS Precinct F/W	1.96.6	N/A	1.96.6 (D0044)	1.96.6	1.96.6	1.96.6
AVOS Central F/W	2.0.12	N/A	2.0.12 (D0044)	2.0.12	2.0.12	2.0.12
AVTSx with AVPM	Bootloader BLR7-1.2.1 Windows CE WCER7-410.2.1 Firmware 4.6.4	N/A	Bootloader BLR7-1.2.1 Windows CE WCER7-410.2.1 Firmware 4.6.4	Bootloader: Not specified. Windows CE: Not specified. Firmware 4.6.4	Bootloader: Not specified. Windows CE: Not specified. Firmware 4.6.4	Bootloader: Not specified. Windows CE: Not specified. Firmware 4.6.4
Key Card Tool	4.6	N/A	4.6.1 (D0044)	4.6.1	4.6.1	4.6.1
VCProgrammer	4.6	N/A	4.6.1 (D0044)	4.6.1	4.6.1	4.6.1
Voter Card Encoder	Spyrus Vote Card Encoder: 1.3.2	N/A	1.3.2 (D0044)	1.3.2	Not Specified.	1.3.2
JResult Client	1.1.3	1.1.3	None (D0044)	None.	None.	None.
GEMS readme.html	Not Present	Present	Not Specified.	Not Specified.	Not Specified.	Not Specified.
Compiled Help	Incomplete/unusable	Present	Not Specified.	Not Specified.	Not Specified.	Not Specified.

Note: The Accuvote-TSx certified in California uses BallotStation 4.6.4, which was approved by Ciber (D0045) for use with GEMS 1.18.24. During the period of the testing, BallotStation 4.6.4 was designated version 4.6.3.12. The version number was promoted to 4.6.4 upon satisfactory completion of the ITA testing.

GEMS Operating Platform

	TTBR GEMS Installation	GEMS Server Administrator's Guide	ITA Reviewed Configuration	NASED N-1-06-22-22-002	Cal. Test Configuration	SoS Certified 2/17/06
Operating System	Microsoft Windows 2000 Server, v. 5.0.2195 SP4 Build 2195	Microsoft Windows 2000 Server SP4	Microsoft Windows 2000 Server, v. 5.0, SP4	Not Specified.	Microsoft Windows 2000 Server, v. 5.0, SP4 "with additional patches for SP5"	Not Specified.
H/W Platform	Dell PowerEdge 2600	Dell PowerEdge 2500 PIII @ 1.13GHz (the “medium” platform)	X86 Family 130,616 KB Ram (*sic*) (D0044)	Not Specified.	Dell PowerEdge 600SC Pentium 4 @ 1.8 GHz	Not Specified.
BIOS	Phoenix ROM BIOS PLUS Version 1.10 A09	Not Specified.	Not Specified. (D0044)	Not Specified.	Not Specified.	Not Specified.
RAM	1 GB	1 GB	128 MB (D0044)	Not Specified.	1 GB	Not Specified.
Graphics Card	ATI RAGE XL PCI	Video card capable of 1024x768	Not Specified. (D0044)	Not Specified.	Not Specified.	Not Specified.
NIC (#1)	Intel PRO/100 S Server Adapter Ethernet 802.3	Intel PRO/100 S	Not Specified. (D0044)	Not Specified.	Not Specified.	Not Specified.
NIC (#2)	Intel PRO/1000 XT Ethernet 802.3	None.	Not Specified. (D0044)	Not Specified.	Not Specified.	Not Specified.
3½ " Floppy Drive	OEM	OEM	Not Specified. (D0044)	Not Specified.	OEM	Not Specified.
Optical Media Drive	H-L Data Storage Model GCC-4240N CD-RW/ DVD-R	24X IDE CD-ROM	Not Specified. (D0044)	Not Specified.	PLEXTOR CD-R PX-W1210S (SCSI)	Not Specified.
Tape Drive	Dell STD2401LW	Internal Tape Backup Unit, 20/40 GB	Not Specified. (D0044)	Not Specified.	Not Specified.	Not Specified.
Local Fixed Disks	4 x 100GB SCSI (NTFS)	3 x 18 GB 10 KRPM Ultra 160 SCSI Hard disk	Not Specified. (D0044)	Not Specified.	20 GB IDE	Not Specified.
SCSI Card	Adaptec 39160/3960D – Ultra160 SCSI	Not Specified.	Not Specified. (D0044)	Not Specified.	Not Specified.	Not Specified.
RAID Controller	DELL PERC 4/Di	4. PERC3, DC, 128MB hard drive controller, 1 internal and 1 internal channel	Not Specified. (D0044)	Not Specified.	Not Specified.	Not Specified.
Sound	Creative	Not Specified.	Not Specified.	Not Specified.	Not Specified.	Not Specified.

Card	SoundBlaster Audigy 2ZS		(D0044)			
IEEE 1394 Controller	Creative SoundBlaster (Driver v 1.82.0, Firmware 0.0.0)	Not Specified.	Not Specified. (D0044)	Not Specified.	Not Specified.	Not Specified.
Printer	HP LaserJet 1022n	HP LaserJet 9000	Not Specified. (D0044)	Not Specified.	HP LaserJet 1020	Not Specified.
	COTS Software					
	TTBR Equipment Configuration Audit	**GEMS Server Administrator's Guide**	**ITA Reviewed Configuration**	**NASED Qualified as N-1-06-22-22-002**	**Cal. Test Configuration Report of 11/11/2005**	**SoS Certified on 2/17/2006**
MDAC	2.8.0.1022.3	2.0	"mdac_typ.exe" (only filename is given.)	Not Specified.	Not Specified	Not Specified.
Java Virtual Machine	MS JVM 5.0	MS JVM 5.0	"msjavax86.exe" (only filename is given.)	Not Specified.	Not Specified.	Not Specified.
JET DB Engine	4.0.9025.0	4.0	Not Specified. (D0044)	Not Specified.	Not Specified.	Not Specified.
File Compression Utility	WinZip 8.1 SR-1 (5266)	WinZip 8.0	Not Specified. (D0044)	Not Specified.	WinZip 8.1 SR-1	Not Specified.
Audio Recorder/ Editor	None.	Adobe Audition v 1.0	Not Specified. (D0044)	Not Specified.	Adobe Audition v 1.0	Not Specified.
VOIP/Videoconferencing client software	Microsoft NetMeeting 3.0	None.	Not Specified. (D0044)	Not Specified.	None.	Not Specified.
Email Client	Outlook Express 6.00.2800.1106	None.	Not Specified. (D0044)	Not Specified.	None.	Not Specified.
Media Player	Windows Media Player 6.4.09.1129	None.	Not Specified. (D0044)	Not Specified.	None.	Not Specified.
mp3 CODEC	Fraunhofer IIS MPEG Layer-3 codec	Lame ACM mp3 CODEC V 0.8.0 – 3.92	Not Specified. (D0044)	Not Specified.	Not Specified.	Not Specified.
PDF Creation Software	Adobe Acrobat Standard v 6.0	Adobe Acrobat Standard v 6.0	Not Specified. (D0044)	Not Specified.	Adobe Acrobat 6.0.0.2003051900	Not Specified.
Optical Media Writing Software	Nero 6 Ultra Edition	Nero 6 Ultra Edition	Not Specified. (D0044)	Not Specified.	Nero ROM Burning Suite, Version 6	Not Specified.
Asian Fonts	None.	Should be installed by Diebold tech prior to delivery	Not Specified. (D0044)	Not Specified.	Not Specified.	Not Specified.

CHAPTER 5

Sufficiency of Documentation

The California Secretary of State requested the Documentation Review teams to determine whether the vendor documentation is ***sufficient.*** Here, we considered whether the documentation adequately supports a county Registrar of Voters' deployment of the electronic voting system (VS) in a manner that empowers the election officials to administer elections accurately, reliably, and with appropriate security and ballot privacy throughout the election processes. Adequate documentation will assist officials in avoiding errors that can cause systemic problems and alert them to strategies they can employ to prevent and detect malicious tampering with the election equipment or vote totals.

Documentation sufficiency for county election purposes turns in part on whether the materials are ***usable*** by the intended audiences. The three key audiences to consider are county election officials, poll workers, and voters.

5.1 Usability Analysis in Voting Systems

Usability analysis is known within computer science and other technical fields as assessments that evaluate whether the materials – hardware, software and documentation – allow the intended human user to perform the expected or desired operations efficiently and confidently. For instance, an automobile that required the ignition key to be inserted on the left side of the steering wheel instead of the right would present American drivers with difficulties in locating the ignition and in inserting the key (using the unexpected left hand). These unexpected departures might also unsettle the driver's comfort level in the car, reducing concentration and pleasure in driving. The auto design world thus takes account of the "human factors" – the ultimate users' expectations, their physical and psychological assets and limitations, as well as the demands of the particular contexts where the automobile "product" will be used.

When designers of a product or its documentation are sensitive to usability considerations, the contexts of its deployment are evaluated along with the actual users' wants, needs, and limitations. Documentation that meets high standards of usability, then, will be tailored to a particular user audience whose needs and wants will be well-researched and well-served For instance, documentary materials discussing the DRE touchscreen voting machine (Diebold's TSx) will not be particularly effective if some hypothetical universal audience is the focus. Rather, county election administrators and technicians should receive different information and possibly a differently organized presentation than that for poll workers or voters. Each target audience has distinct needs, owing to its different duties with regard to elections.

Usability analysis in elections has thus far tended to focus on the voter. For instance, a Brennan Center report reviews studies documenting the statistical differences between different types of voting systems with regard to the consequences for voters' ability to complete a valid ballot.[34]

In the analysis that follows, we focus predominantly on the usability of vendor-supplied electronic format documentation with regard to the two target audiences who play critical roles in election administration: county election officials and poll workers. These audiences have received little attention in the nascent election usability field, with far more concern being placed on voters' needs. Yet, as Quesenbery notes, voters' needs cannot be well-served if election officials and technicians are not well-served in preparing the election. [35]

5.2 Usability of Documentation by Election Officials

The conscientious county election manager, like managers elsewhere, desires to demonstrate a quality job performance in assigned work duties. Given the non-negotiable election calendar, efficiency and timeliness of performance matters can matter greatly. Greater media and public scrutiny of election operations may lead to significant job stress, because of a perceived need for election administrative operations to move very smoothly. If unexpected technical events or administrative problems with, for instance, ballots occur, a cascade of problems can ensue simply because the calendar dates for other tasks are dependent upon effective completion of predicate tasks. The election administrative process, then, especially in urban counties, requires a series of intersecting functions to meet precisely on time with little more flexibility than that of trapeze artists. The consequences of failed elections can not only mean job sanctions including termination, but the potentiality of individual civil or criminal penalties. Thus, stakes are very high.

In order to manage an election that produces prompt reporting of accurate, verifiable results on relatively new electronic voting equipment, officials will be often find themselves facing an intense learning curve. Questions and concerns will arise frequently. Given the election calendar fast, accurate responses are needed to the questions about the VS technology, ranging from supplies and maintenance to intensive Election Day operations.

This understanding of election officials' managerial situations leads to several criteria for evaluating the adequacy of VS documentation:

- ***Speed of use***: Can answers to questions be found quickly with little wasted time scanning irrelevant material?
- ***Accuracy and consistency***: Does the documentation provide one answer that is correct, or several conflicting answers?
- ***Clarity***: Is the documentation written with unambiguous, relatively easy to understand language?
- ***Risks***: Where a given procedure holds great risks for achieving a successful election if not performed precisely right, does the documentation flag it with visual cues and exceptionally clear writing?

[34] The Brennan Center of Justice report, T*he Machinery of Democracy: Usability*, reviews a the literature on voter usability. *See* www.brennancenter.org/dynamic/subpages/download_file_36340.pdf.

[35] *See* Whitney Quesenbery, *Position Paper for UPA Voting and Usability Workshop 2004, found at* www.upassoc.org/upa_projects/voting_and_usability/workshop_2004: "We need to consider not only voters, but everyone in the elections process: poll workers (and their materials and training), elections officials (and the usability of the tools they use to create a ballot)."

- ***Effective support for core election objectives***: Given the critical objectives of election accuracy, security, reliability, and ballot secrecy, does the documentation effectively educate and support election officials in managing election operations related to the VS so that high standards in each of these areas can be achieved?

In reviewing the user or operational manuals Diebold provides, these five criteria form the baseline for documentary usability evaluations. This report focuses on three subsets of election operations documents as exemplars of the Diebold documentation: those concerning GEMS; TSx touchscreen support, and optical scanning—both precinct count and central count.

5.2.1 Speed of Use

Does the documentation allow election officials to locate answers to their questions quickly?

Macro-Organizational Usability Considerations Diebold has generated a very large number of operating manuals, which it tends to divide into groupings it terms "suites." As concerns VS components, the suites are not simply a hardware manual and a software manual, or an election official's administrative operational manual and the maintenance/hardware manual. Instead, Diebold generally supplies a *multitude* of manuals. Yet when inventorying the manual suite in a given introduction, it is not unusual for Diebold to excerpt the list and exclude some manuals that provide valuable information not repeated elsewhere. The GEMS Reference Guide, for instance, is often not mentioned in the list of GEMS manuals at the front of a Manual introducing the system documentation.

Significant problems attend this proliferating approach to documentation. The logic of where to look for particular issues, explanations and information is not readily apparent. One can comb through several manuals without locating any information on the point in question. Second, instead of having only a few well-organized, well written manuals that election officials might begin to master as far as internal logic and content, it seems that the Diebold documentation effort has become one focusing on producing a quantity of manuals rather than their quality or overall usability.

For instance, the GEMS 1.18 operators' or users documentation includes:

- Election Administrator's Guide, Rev. 8.0 (543 pages).
- Product Overview Guide, Rev. 2.0, (13 pages).
- Reference Guide, Rev. 8.0 (355 pages).
- System Administrator's Guide, Rev 6.0 (95 pages).
- User's Guide, Rev. 12.0, (281 pages).
- JResult Client 1.1 User's Guide, Rev. 1.0, (28 pages).

In rough numbers, this is a total of over 1300 pages spread between six manuals. This team concludes that the documentation is unusable for reaching speedy answers.

At the beginning of several manuals Diebold presents the GEMS documentation in this manner:

> 1. *GEMS Election Administrator's Guide*, which provides a comprehensive description of all election management tasks involved in configuring an election using Diebold … election products, including the GEMS election management software and AccuVote-TS and AccuVote-OS voting and ballot counting devices.
>
> 2. *GEMS Product Overview Guide*, which provides an overview of Diebold … election products and product documentation.

> 3. *GEMS Reference Guide*, which provides a comprehensive description of the concepts involved in GEMS functionality.
>
> 4. *GEMS User's Guide*, which provides a comprehensive description of the implementation of GEMS functionality.
>
> 5. *GEMS System Administrator's Guide*, which provides a comprehensive description of all technical administrative activities involved in the usage of GEMS software and GEMS clients.

For county election managers, or anyone else who needs to become technically proficient in operating or managing GEMS, the documentation divisions as between the various manuals are not conceptualized well or presented accurately. Their division is particularly frustrating from the standpoint of operational management and trouble-shooting. Hence, a local official in charge of a particular managerial task (for instance, absentee ballots to be tallied on a central count optical scan system) would not find the instructions in one or two manuals but in parts of five separate GEMS manuals, and most likely needing to use three manuals repeatedly which range between 280-540 pages. She would also need to research the suite of AV-OS manuals, plus possibly the Digi-port manual and still others.

Not only are the manuals' division of information not logical from an operational standpoint, but the information needed from other manuals is not cross-referenced or well-indexed. A conscientious absentee ballot manager would need to generate his or her own manual in a cut-and-paste manner – if Diebold's effort to protect its manuals from photocopying did not interfere.

For Central Count AV-OS, Diebold documentation suggests this organization to its literature:

> AccuVote-OS device are described in the *AccuVote-OS Hardware Guide*, including the installation of AccuVote-OS Central Count firmware. For information on the configuration of the AccuFeed for use with the AccuVote-OS, refer to the *AccuFeed Hardware Guide*. For information on administrative considerations in the use of AccuVote-OS Central Count, refer to section 9 *Absentee Processing* the *GEMS 1.18 Election Administrator's Guide.*

Unfortunately, not all the information that is needed or relevant to setting up and managing AV-OS Central can be found in these three AV-OS manuals..

If an official sought the ***error message list*** for optical scanning, the listing would run numerous pages. But he would discover that it is not ordered alphabetically, by function, by election phase, or by any other discernible criterion. In the manual's text, the chapter 8 heading (which also is stated in the Table of Contents/Index) does not mention it as the Error Message chapter but instead lists it as the *Ballot Return Message*:

> **8. *Ballot Return Messages***
> This chapter lists all possible ***error messages*** that may occur in the course of ballot testing and counting. Each message is listed with the probable error cause as well as a recommended solution. Any ballot conforming to the ballot return criteria defined under the Reject Settings tab in the AccuVote-OS Options window in GEMS is returned by the AccuVote-OS. . . . *(emphasis added).*

This form of indexing requires that an official already know the particular terminology used by the vendor in order to discover critical information, Unfortunately, a large number of Diebold operational/user manuals lack an alphabetical index with information cross-listed using several key words, including vendor specific names, technical nomenclature and more common operational or election vernacular.

5.2.2 Accuracy and Consistency

Does the documentation provide one name for a component or process, or several conflicting answers? Are the operational facts of the equipment presented accurately?

Apparently, this vendor does not desire election official reliance on the accuracy of its manuals, as indicated by a disclaimer of warranty. Rather surprisingly, this vendor appears to include at the front of every operational or customer manual a warranty disclaimer. The most recent version was found in the *Readme* file that the vendor supplied with the portion of TDP files it submitted to the TTBR in mid-July. This 2007 *Readme* file may reflect the most recent version of the documentation disclaimer:

Disclaimer of Warranty

> The ***information in this document is provided 'as is' and without warranty***. Diebold Election Systems will not be liable for any incidental, consequential, or other damages of any type or nature, resulting from the provision or use of the information contained herein. All information is subject to change at any time without notice. ***Users of this document assume sole responsibility for their use of the information contained herein, as well as any products, software, or other materials that may be provided by Diebold Election Systems***. Care should be exercised by such users to assure compliance with all applicable laws, rules, and regulations. *(emphasis added).*

Whether this language is unenforceable as a matter of California or other law is a question that the Secretary of State may want to explore. Non-lawyer election officials may assume language has been vetted and is legally enforceable since it appears in a document that presumably has been reviewed by certification authorities (though the enforceability of warranties would likely be well beyond the scope of certification reviews).

Examples of inconsistent and confusing parts nomenclature:

AV-OS: Precinct Count Optical Scan Hardware Guide: *Multiple, possibly inconsistent names for the ballot box compartments.* In addition to the "main" compartment, additional compartment names include "secondary," "alternate," "auxiliary," and "side," for a total of five names. While the documentation states there are four doors and one compartment has two doors, it does not state how many compartments are located in the scanner's ballot box. Some examples *(with emphasis added)*:

> Sorted ballots are dropped into the *secondary compartment* of the ballot box if the AccuVote-OS is installed in the ballot box . . . .
>
> **4.3.2. Separating ballots into the *alternate ballot box compartment***
> The AccuVote-OS may be programmed to sort ballots encountered any of the conditions selected. . . . Sorted ballots are dropped into the *secondary compartment* of the ballot box if the AccuVote-OS is installed in the ballot box….
>
> **3.2.7. Ballot box compartments**
> The *four doors* that access the ballot box compartments are locked using either of the ballot box keys. All ballot box compartments should be verified as being empty prior to voting begin. A small opening on the upper left side of the ballot box provides access to an *auxiliary compartment*. . . . The door on the lower left side of the ballot box also provides access to the *auxiliary compartment*, but this door should only be opened to remove ballots from the auxiliary compartment at the end of election day or to be counted on the AccuVote-OS. The back door of the ballot boxes is designed to allow the removal of ballots . . . or in case of an AccuVote-OS failure (where ballots are transferred to the *side compartment*).

3.2.9. Separating ballots in the ballot box
Ballots, such as write-in or blank ballots, may optionally drop into the *secondary compartment* within the ballot box.

Inconsistencies not only lead to miscommunications but also can be repeated in poll worker and other election official training.

5.2.3 Clarity

Is the documentation written unambiguously, so it is relatively easy to understand?

Speed in using manuals can depend not only on the quality of indexes but also on the clarity of the writing in the discussion desired. Unfortunately, most Diebold user manuals were pervaded with poorly edited, unnecessarily lengthy and confusing sentences. While election officials are rarely IT professionals, the manuals tended to rely on technical jargon that could easily detract from the larger election administrative or mechanical points that needed to be understood.

Virtually all of the manuals included one relatively well-edited Introduction. Each of these introductions appeared to have been reproduced from marketing information. Without exception, they touted the ease of use and high performance of the Diebold line of products. Had the balance of the manuals been edited to the same degree as these Introductions, the clarity and usefulness of the writing would have improved. For all manuals other than the AV-OS Hardware manual, this introductory passage seemed to be the only portion of the writing that was edited for clarity and persuasion. The contrast between the introductory overview and the operating instructions and explanations seems quite sharp and ultimately detrimental to the effectiveness of the manuals

<u>Examples of well written passages or manuals</u>:

- The AV-OS Hardware Manual is a relatively well written resource, with reasonably good internal organization and clear writing.
- The GEMS 1.18 Reference Guide includes some very well written definitions in its Appendix A: Glossary, that avoid dependence on using the word sought to be defined:

  Closed primary: A primary election in which voters vote on ballots containing only races corresponding to their political party as well as any non-partisan races in the election.

  Export: The composition of election and election results information into an ASCII file format.

  Election Summary report: A report summarizing election results by race, across the entire jurisdiction, presented according to customization criteria.

<u>Most other manuals have significant problems with language precision and lack of clarity; they</u>**:**

- provide definitions with dependence on using the word sought to be defined: **[36]**

  Monitor Script: A JResult Client configuration, defined in terms Monitor Script Properties, in turn defined in terms of sets of reporting sets and precincts or districts.
  Monitor Script Properties: Monitor Scripts are defined in terms of Monitor Script Properties, which

[36] 2005 GEMS 1.18 Reference Guide, Glossary.

are in turn defined in terms of sets of reporting sets and precincts or districts

- provide confusing and imprecise definitions that fail to clarify the differences between related but distinct words:

  ***Ballot*:** A Ballot refers to a rotated ballot style. A single card comprises all language variants for the card.
  Card: A rotated, physical document containing a unique set of races. One or more cards comprise a single card style. A single card comprises all language variants for the card.
  Card Style: A physical document that is contained within a ballot style; a ballot style may contain one or more card styles. A single card style comprises all language variants for the card style.
  Deck: A set of ballots processed in Central Count, delimited by Batch Header or Batch Start cards.

  The Glossary provides no entry for ***"batch"*** although the documentation sometimes uses the words "deck" and batch interchangeably, and other times with apparently distinct meanings. The usage sometimes appears to suggest that a *"**deck"*** is the electronic representation of a physical ***"batch"*** of ballots processed in the central count scanning system, but the documentation lacks consistency in usage, and the definition provided here does not support that distinction.

- miss an opportunity for promoting mechanisms for checking tabulation work with an aim for achieving greater accuracy

  Ballot Audit: A function allowing the review of ballots uploaded from AccuVote-TS units.

  Ballot audits can occur with optical scanning processes as well, and arguably should occur with all tabulation equipment.

<u>Operational user manuals display problems with clarity, precision and jargon throughout</u>. A few examples include:

AV-OS Precinct Count[37]

3.2. Ballot tallying *[describing how AccuVote-OS ballots are counted and tallied]:*
For every ballot encountered, the Times Counted counter is incremented for the ballot as well as the Times Write-In counter if the ballot contains at least one write-in candidate selection in a non-overvoted race.

3.3.5. Shadow races
A race may be configured to automatically tally to reporting districts that intersect the district over which the race runs, or to voter groups with which partisan ballots in which the race runs are affiliated. A race is defined with Type Shadow with district, voter group, and all other parameters of a candidacy, with as many Shadowed races linked to the Shadow race as necessary to satisfy reporting requirements

3.5. Programmable ballot sort conditions
[AccuVote-OS can be programmed to sort ballots] encountering any of the conditions selected under the Sort Ballots With column under the Reject Settings tab in the AccuVote-OS Options window in GEMS.
Sorted ballots are dropped into the secondary compartment of the ballot box if the AccuVote-OS is installed in the ballot box, otherwise, if ballots are being counted in batch mode with the AccuFeed installed, a sorted ballot is dropped into the AccuFeed outfeed tray, a message is displayed on the

[37] 1.96 User's Guide (2005).

> AccuVote-OS LCD indicating that a sort condition has arisen, alternating with a prompt to press the Yes button and continue.
>
> **7.8.2. Tallying ballots with exception conditions**
> In section *7.8 Ballot rejection,* you are presented with information pertaining to the processing of ballots that are returned as a result of meeting certain ballot return conditions programmed in GEMS. This section explains in simple terms how ballot tallying is affected ballots with any of these conditions are accepted by the AccuVote-OS, either because the election has not been configured to return ballots with the said return condition, or ballots with this condition have been encountered, but fed into the AccuVote-OS in override mode.

Other problematic examples from the same precinct count AV-OS manual include:

> The Times Counted counter is incremented for every race on the ballot, as well as the Total Votes counter for every candidate and write-in position selected in every nonovervoted race.
>
> For every open primary ballot with overvoted crossover races encountered, the Times Counted and Times OverVoted counters are incremented for the ballot as well as the Times Write-In counter if the ballot contains at least one write-in candidate selection in a non-overvoted, nonpartisan race
>
> The AccuVote-OS may be programmed to return ballots encountered any of the following conditions selected under the Return Ballots With column under the Reject Settings tab in the AccuVote-OS Options window in GEMS.

Central Count Optical Scan manuals fail to distinguish between the batch and the deck**:**

> *Batch* numbers are pre-assigned from *Batch Header* cards, where GEMS assigns the batch number coded onto the Batch Header card as it is fed. It is not possible ... to assign a Batch Start card which has already been used unless the original *batch* is deleted from the database. The AccuVote Ender card is used to end a batch, at which point the batch is committed to the GEMS database. If the counting of a batch is interrupted (ie. the connection to the host computer is lost) the contents of the *deck* are also lost.
> *[More reasons than this... Ed.]*

Frequently, the documentation fails to use common titles for events or conditions, rendering the user unable to effectively use indices or lists of issues:

> **10.2. Equipment *recuperation***
> If the AccuVote-OS or memory card malfunctions and requires replacement. . . . .

5.2.4 Risks

Where a given procedure holds risks to a successful election if not performed precisely correctly, does the documentation flag the point with visual cues and exceptionally clear writing? Is contingency planning discussed adequately?

This team would suggest that the vendor accorded insufficient attention to the risks potentially accruing to election employees personally and individually if the VS vendors omit disclosures of risks to quality election task performance. Additionally, we believe that the documentation should augment election workers' knowledge of how to protect themselves from the possibility of rogue employees attempting to leave evidentiary trails suggesting that another worker had engaged in wrongful conduct.

These risks and the mitigation strategies should be disclosed for employee protection.

A clearly written notification of a major precinct count optical scanning risk is stated here with practical advice designed to mitigate the risk:

> **7.6. Replacing a full ballot box**
> Each ballot box holds up to 1500 ballots in each of the main compartments. Spare ballot boxes should be provided to polling places anticipating heavy voting. We recommend checking the contents of the ballot box when the ballot counter reaches 1000, and using the following procedure to replace the ballot box once it is full.

Unfortunately, the note does not include a warning flag or other distinctive visual cue. The manual presents a photograph, however, that does assists in visualizing the situation and point to recall.

Overall, the Diebold manuals are generally bereft of warning boxes, special flags or colors for dangers and risk factors, or other techniques for emphasis. Many critical risk factors are not mentioned, or are understated, buried in the midst of long passages of text.

The documentation inadequately addressed some serious risks or did not disclose them at all:

- ***Election results database growth.*** GEMS use of the JET engine means the database is limited to 2 gigabytes; database corruption is a well documented risk thereafter.[38] Given the risks to election database integrity, all factors that can cause rapid database growth should be disclosed with appropriate mitigation strategies. Currently, the Diebold optical scanning manuals we reviewed did not even advise that the GEMS database file (containing size information) should be monitored during central count scanning.
- ***Central count scanning.*** The scanning operations can sometimes result in defective data being uploaded into GEMS. The GEMS manuals include some instructions for recognizing and monitoring for the need for a batch/deck deletion, but they fail to note the serious risks for election data from operator errors, and omit needed mitigation strategies. The documentation also sidesteps offering careful instructions on how to guard against duplicate scannings of a ballot batch and failures to re-scan a deleted batch.[39] To the degree that different types of batch start cards can be used for this internal auditing and tracking of batches, improved election accuracy can result. Thus, these and other strategies should not only be disclosed but effectively taught via the documentation. Additional strategies to improve accuracy and avoid risks could involve instructions on using scanning audit logs effectively and creating backup data points by periodically burning database records during scanning and other ballot tabulations.
- ***Presence and Use of Modems.*** In both the TSx and AV-OS, modems generate certain risks to election results and to the reliability of the VS equipment, as discussed in the Diebold Red Team and Source Code reports.
- ***Audit Log information****:* These logs offer substantial value to security and accuracy values, but unless the documentation explains how to use them and the various purposes for which they are relevant, their presence is nearly meaningless. Their value extends from discerning some types of tampering, to identifying system failures or problems and operator errors, to trouble-shooting and improving election operational performance.

[38] *See, e.g.,* Diebold Source Code Team report.

[39] The Cuyahoga Collaborative Public Audit discovered deleted ballot batches that had not been rescanned, and batches that had been scanned more than once. The Final Report is located at www.csuohio.edu/cei/.

- ***Networks***: The Diebold documentation made available for this review sidestepped the risks of data dregradation, the role and specifications of appropriate network stress testing, and major risks to the GEMS server created by the network connections.
- C***oncurrency issues and limitation.*** JET presents the possibility of concurrency problems that can lead to data degradation or system failures. Diebold documentation remains mute on this matter.
- ***Disclosures of known VS vulnerabilities.*** Published studies and election administrative experience has developed a set of vulnerabilities for various components of the Diebold VS. Operational mitigation strategies then become key protections for election integrity. But this vendor fails to disclose known vulnerabilities, and fails to offer appropriate mitigation strategies.

5.2.4.1 Contingency Planning

Step-by-step procedures covering election administration under optimal circumstances are essential. Equally essential are detailed strategies for handling problems that arise. The Diebold customer documentation offered helpful strategies for dealing with contingencies such as responding to unexpected polling place supply shortages on Election Day, cold-swapping voting device batteries in response to isolated power failures, and physical transportation of memory cards when remote upload of voting data fails. In areas in which the voting systems themselves appear to be malfunctioning, or when possible tampering is detected, however, this vendor's documentation offers few prudent and realistic instructions for troubleshooting, mitigating, recovering and reporting.

In order to effectively handle adverse conditions, election officials need precise information on the state of the voting system, on its recovery features and on the level of fault tolerance that the system reliably exhibits in specific situations. The Diebold documentation reviewed for the TTBR provides little guidance to election administration officials on recovering from adverse events and mitigating the impact of failures, errors and malicious actions. The response, recovery and mitigation instructions presented in the documentation are often inappropriate, incomplete, obvious or impractical.

As detailed below, several contingency response procedures in the documentation rest on dubious assumptions about the certainty with which one can determine the precise state of system components in the aftermath of system failures and other adverse events. Such assumptions may lead to responses that can cause the situation to deteriorate by directing that election operations proceed without verifying that executable code and data structures are intact following a system failure or security breach. Some of the vendor's proposed contingency plans appear to risk propagation of malicious code.

In cases where malicious intrusion into voting systems is suspected, the manuals offer little information about the need to isolate equipment to contain the threat and preserve a device intact for forensic examination. The manuals offer no guidance whatever on what general sorts of forensic investigations would be appropriate.

Dubious Contingency Plans The following examples illustrate the wide range of questionable contingency response information contained in Diebold's customer documentation. They make categorical assertions of questionable technical accuracy or prudence, instructing workers to proceed with potentially damaged or compromised equipment, or reassuring workers about the reliability of the system state.

- "The technician should replace the hard drive and attempt to extract the contents of the failed hard drive to the replacement drive. If this restoration activity is successful, then the integrity of the

GEMS installation and election configuration should in no way have been compromised."[40]

- "The AccuVote-TS cannot be voted or rendered functional in a meaningful way unless a programmed memory card is installed." [41]

- "Vote totals cannot be accumulated to an AccuVote-OS memory card other than with the availability of AccuVote-OS ballots. It is possible that an unauthorized party manufacture *(sic)* ballots, but without specific knowledge of ballot specifications and electronic ballot images generated by the GEMS election management software, it would be unlikely."[42]
- "If ballots are available to the unauthorized party, and ballots are marked, it will not be possible to tally results without the availability of an AccuVote Ender card. If an AccuVote Ender card is present, results may then be tallied on the memory card."[43]

- "If power failure results in damage to the voting machine as a result of a lightning strike, then the voting machine must be replaced. In case of an either an AccuVote-TS or AccuVote-OS unit, the memory card should be removed from the damaged unit and installed in a replacement unit, and voting continued."[44]

- "Erroneous configuration or behavior should result in the immediate replacement of the voting device. [...]Since the tallies of official ballots cast on the device are resident on the memory card, the seal number should be recorded of the failed unit, the memory card removed from the device, the memory card then installed in the replacement unit, a new seal number applied, and recorded."[45]

- "If a voting machine is damaged at a polling location, then the voting machine must be replaced. In case of an either an AccuVote-TS or AccuVote-OS unit, the memory card should be removed from the damaged unit and installed in a replacement unit, and voting continued, provided that the memory card has remained intact."[46]

From a technical standpoint, some guidance the manuals offer is reasonable, but by no means complete. For instance, Diebold recommends responses for events where evidence of tampering or system failure has arisen, but these instructions are missing important additional steps. Examples include:

- "If unauthorized software is detected on the GEMS server, that software should be removed immediately. Software uninstallation should be performed by qualified IT staff, upon approval by Diebold Election Systems, Inc."[47]

- "In the event that unauthorized physical access to the GEMS server is detected, either as a result of observing an attempt at physical access or by reviewing the operating system audit trail, it is essential that physical security be enhanced in the environment of the GEMS server. Physical security should be enhanced at least for the duration of the election lifecycle."[48]

[40] *GEMS 1.18 Election Administrator's Guide, Revision 8.0,* p. 16-59.

[41] *GEMS 1.18 Election Administrator's Guide, Revision 8.0,* p. 16-61.

[42] *GEMS 1.18 Election Administrator's Guide, Revision 8.0,* p. 16-62.

[43] *GEMS 1.18 Election Administrator's Guide, Revision 8.0,* p. 16-62.

[44] *GEMS 1.18 Election Administrator's Guide, Revision 8.0,* p. 16-66.

[45] *GEMS 1.18 Election Administrator's Guide, Revision 8.0,* p. 16-60; statement is repeated in reference to the AccuVote-OS on page 16-62.

[46] *GEMS 1.18 Election Administrator's Guide, Revision 8.0,* p. 16-65.

[47] *GEMS 1.18 Election Administrator's Guide, Revision 8.0,* p. 16-59.

[48] *GEMS 1.18 Election Administrator's Guide, Revision 8.0,* p. 16-58.

Other contingency instructions are obvious or unneeded, for example:

- "If power failure results in damage to the GEMS server as a result of a lightning strike, then the appropriate components of the GEMS server must be recuperated."[49]

- "Damaged Voter Card Encoder units that are no longer operational should be replaced with replacement Voter Card Encoder units."[50]

- "In the event that a critical employee in the election management process becomes suddenly unavailable, it is essential that an alternate qualified employee be located and trained immediately. [...] Initially, a replacement employee occupying a critical position should be provided as much assistance as possible from related staff positions."[51]

- "If power failure occurs during election closing, memory cards should be driven in to the election administration office in place of attempting to upload memory cards."[52]

- "AccuVote-OS units should be monitored in the course of election day in order to ensure their continued ability to count ballots."[53]

- "In the event of delay of results accumulation to the GEMS server, an announcement should be made to the public pertaining to the delay of results pending resumption of power."[54]

Some contingency response plans are impractical or legally impermissible. For example:

- "If memory cards have been lost, the election must be re-scheduled."[55]

- "If the AccuVote-TS unit with installed memory card disappeared from a voting location in the course of or at the conclusion of election day, but prior to uploading, then all votes on the machine will be lost, and all voters at the polling location will have to be called in to re-vote. All machines present at the polling location may upload results at the end of election day, barring the missing unit, and once all voters at the polling location have completed the repeat vote, the new results are uploaded to the GEMS server after the original results for the vote center are cleared in the GEMS database."[56]

- "If both the AccuVote-TS unit and installed memory card are damaged in the course of or at the conclusion of election day, but prior to uploading, then all votes on the machine will be lost, and all voters at the polling location will have to be called in to re-vote."[57]

[49] *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, p. 16-57.

[50] *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, p. 16-64.

[51] *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, p. 16-57.

[52] *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, p. 16-66.

[53] *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, p. 16-62.

[54] *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, p. 16-57.

[55] *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, p. 16-56.

[56] *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, p. 16-61.

[57] *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, p. 16-65; statement is repeated in reference to the AccuVote-OS on page 16-66.

5.2.5 Effective support for core election objectives

Given the critical objectives of election accuracy, security, reliability, and ballot secrecy, does the documentation effectively educate and support election officials in managing election operations related to the VS so that high standards in each of these areas can be achieved?

5.2.5.1 Poll Worker Support

Diebold documentation does not include a dedicated poll worker guide for either type of polling location voting equipment. Rather, it includes manuals designed for election officials to use in constructing a poll worker guide. These vendor guides to creating a local poll worker manual are deficient in numerous ways. One key reason this is not an acceptable vendor approach for achieving quality local election support is that local election officials are largely unfamiliar with usability criteria for manuals. It would be an unusual election official who had experience writing effective manuals about complex technical matters for a non-technical audience of various literacy levels. Thus, self-sufficiency in developing poll worker manuals or training would be illusive.

A quality ***template*** (with an unlimited, no fee license) for a poll worker manual would seem to be a reasonable expectation of each VS vendor. The Diebold poll worker manuals cannot and do not function as such a template. Each of them is poorly organized; include a range of technical information not suitable or needed for the poll workers; are not clearly written; fail to stress or even explain the security role of the poll workers effectively; and seem obviously not developed by anyone who has experience in teaching poll workers. These manuals cannot function as quality written materials in support of teaching election workers.

5.2.5.2 Accuracy and Verifiability of Election Results

Some GEMS programming options that are detailed in the manuals can promote voter accuracy and election administrative improvements -- if they were more widely known and used effectively:

GEMS *[Programming options for optical scanning]*

7.8.1. Programmed ballot return condition: to return ballots according to special voting “conditions.”
The options are:
1. Overvoted ballots
2. Undervoted ballots
3. Blank voted races
4. Blank voted ballots
5. Overvoted crossover races
6. Overvoted straight party races

GEMS *[maintains tallies or “counters” not widely known that can promote auditing and improvements]:*

<u>Counters</u>
The following counters are maintained in the process of counting and tallying AccuVote-OS ballots. For each ballot:
1. ***Times Counted*** represents the total number of cards counted, and is incremented for every card counted
2. ***Times Blank Voted*** represents the total number of cards with blank voted races, and is incremented for every card with one or more blank voted races.

Ballot Processing
3. ***Times OverVoted*** represents the total number of cards with overvoted races, and is incremented for every card with one or more overvoted races.
4. ***Times UnderVoted*** represents the total number of cards with under voted races, and is incremented for every card with one or more undervoted races.
5***. Times Write-In*** represents the total number of cards with write-in votes, and is incremented for every card with one or more write-in candidate selections.

For each race:
1. ***Total Votes*** is maintained for every candidate and write-in candidate position, and is incremented for every valid vote assigned to the candidate or corresponding write-in position
2. ***Times Counted*** represents the total number of times the race was counted, and is incremented every time the race was encountered
3. ***Times Blank Voted*** represents the total number of times a blank voted race was counted, and is incremented every time a blank voted race was encountered
4. ***Times OverVoted*** represents the total number of times an overvoted race was counted….

A misused Precinct Header card can disrupt election accuracy and is insufficiently flagged.

5.2.5.3 Reliability

The rate of failures in technical equipment is often referred to as its "reliability." This point is crucial for VS as failures in a component can disenfranchise voters or disrupt an election. Metrics for component failure rates are not provided in the documentation, and it appears the vendor does not suggest that the jurisdiction keep failure records of components.

Reliability issues can be more effectively managed if full disclosure of risk factors occurs. Some key risks that affect the reliability of the VS are discussed in section 5.2.4 above.

The Diebold VS Hardware manuals often include sound suggestions and guidance for maintenance issues that can affect the reliability of VS components. .

Poll worker guides are possibly at their strongest in the diagrams and instructions on how to set up and close down voting devices, which also relates to VS component reliability.

5.2.5.4 Ballot Secrecy

We examined the vendor documentation for indications that the vendor was effective in identifying ways to promote ballot secrecy, including by flagging risk points for compromising a voter's interest in maintaining the confidentiality of his or her ballot choices. The discussion that follows leaves to the other Diebold teams an assessment of the degree to which a voter's selections may be traced back to a particular individual via technical means and instead focus on the ballot secrecy provided to the voter for period during which the ballot is being marked and cast.

AccuVote-TSx The AccuVote-TSx unit has two plastic flaps or doors that swing away from the front of the device to create visual barriers to the left and right of the touchscreen where the visual ballot is displayed. These are intended to reduce the visibility of the touchscreen to observers on either side of the voter. The primary visual barrier protecting the front of the screen is the voter's body.

The documentation refers to the doors (called "privacy panels") as the safeguard against observers seeing a voter's votes as they are cast.[58] The materials do not discuss ways to improve or promote the privacy doors' use for better assuring privacy. Further, one critical consideration for TSx ballot privacy -- physical arrangement of the machines in the polling place – is accorded cursory attention, with only a suggestion that the local officials provide a physical layout.

The documentation does highlight an important feature available to voters who select an audio ballot. These voters are given the option of having the touchscreen remain entirely blank as they make their selections. This feature clearly augments the ballot secrecy of the audio-only ballot.

In addition to the documentation's omission of privacy issues that arise for the visual ballot voter that are not addressed by the privacy panels, it further overlooks the role that small physical size can play in the voter's ballot being seen as it is being marked, or the choice of larger typeface, or the angle that the screen is set. The documentation does not offer any guidance on the degree to which magnified ballots might require additional steps to achieve ballot secrecy. Clearly, a voter should not have to make a trade-off between ballot legibility and ballot secrecy.

Many problems of the voter's selections being observable may be mitigated by careful physical configuration of the machines or the introduction of additional, freestanding visual barriers. An election administrator or poll worker attempting to increase the privacy of voters using the AccuVote-TSx at a polling place, however, could not rely on the documentation provided with the voting devices for guidance. Such problems may be aggravated during early voting, when small numbers of voting devices may be located in facilities housing other public activities, and which are not configured exclusively for voting.

Other documentation that might be helpful in advancing voter secrecy when using the AccuVote-TSx would be instructions on how a poll worker may assist a voter with a question without viewing the touchscreen. A mechanism by which a voter could temporarily blank the screen while seeking aid from a poll worker might also be of value.

One statement in the Diebold customer documentation gives an indication of its overall treatment of the ballot secrecy issue. In discussing measures to take when there is a concern that someone has been able to manufacture multiple, fraudulent voter access cards, the *GEMS 1.18 Election Administrator's Guide* states:

> *AccuVote-TS units at the polling place may be configured in a manner that assures voter privacy, but allows poll workers to detect attempts made to perform repeat insertions of voter access cards into the AccuVote-TS smart card reader*.[59]

The documentation does not offer any suggestion as to how this might be done. It simply states that it is possible to set the DREs up so as to observe the insertion of smartcards, and that it should be done in certain situations. Encouraging poll workers to keep an eye on voters activities, somehow without observing their votes or otherwise intimidating them, to address a supposed security breach may do more to compromise ballot privacy than to augment security.

Any testing-based assessment of ballot secrecy is complicated by the difficulty in quantifying degrees of "ballot secrecy" with reference to the human observer. The Wyle report on the AccuVote-TSx does not describe any testing conducted to determine observer proximity and viewing angles that permit a voter's

[58] "The AccuVote-TSX privacy panels are maintained in an open position on election day, in order to protect the voters' privacy in the course of voting." *AccuVote-TSx Hardware Guide, Revision 8.0,* p.2-1.

[59] *GEMS 1.18 Election Administrator's Guide, Revision 8.0,* p. 16-64.

selections to be seen, or give details of the physical configurations that were found to provide adequate ballot secrecy. The nearly limitless array of venues in which voting takes place also hinders standardization and quantization of any testing methodology.

Accu-Vote-OS Assuming that voters are afforded reasonable privacy for filling-out paper ballots, the degree of ballot secrecy depends on the support afforded voters using precinct-based Accu-Vote-OS devices – particularly when the voter places the ballot into the scanner. The documentation discusses the use of opaque sleeves to cover the paper ballot while it is being fed into the AV-OS.[60] It is less effective in describing the poll worker's procedures to maintain ballot secrecy if the scanner jams or returns the ballot. The poll worker manual for AV-OS should stress these procedures and the importance of not observing a voter's selections, such as not removing the sleeve before feeding the ballot. Voter privacy would be advanced by clear warnings of these risks in the documentation, and by encouraging the creation of local polling place policies or mechanisms to reduce the opportunities to view a returned ballot, including from a line of waiting voters.

[60] "Secrecy sleeves are used to cover the marked contents of the ballot while the ballot is fed into the AccuVote-OS, maintaining the secrecy of the voter's selections on the ballot." *AccuVote-OS Hardware Guide, Revision 5.0*, p. 2-4.

CHAPTER 6

Security

We evaluated the security policies presented in Diebold's customer documentation, their internal documentation and the documentation submitted to ITAs as part of the Technical Data Packages with which we were provided. While there are elements of sound policies throughout, we found several significant problems, including:

- Inconsistent security policies in different documentation sets.
- Problematic statements and assurances in the documentation distributed to customers.
- Failure to implement reasonable and consistent security configurations for systems delivered to customers.

6.1 Inconsistent Security Policies

Among the information that the VSS requires as part of the confidential Technical Data Package (TDP) that the vendors submit to testing authorities during the qualification testing process are "mandatory administrative procedures for effective system security."[61] This information is crucial to assessing the security of a voting system because security vulnerabilities have as much to do with how systems are used and administered as with the systems themselves. A highly-secure system may be subject to all manner of attack if it is not operated according to sound usage policies. Likewise, risks due to holes in a system's security may be mitigated by strict adherence to well-designed usage policies.

Diebold submitted extensive materials labeled as *Appendix X* as part of its GEMS TDP.[62] The *System Functionality Description* section of the GEMS TDP states that the mandatory administrative procedures for GEMS are contained in TDP *Appendix X* and in the *GEMS 1.18 Election Administrator's Guide*.[63] The *Election Administrator's Guide,* however, is distributed to customers as part of the GEMS documentation set, while *Appendix X* is part of the confidential TDP that customers do not receive. No document describing a client security policy similar to that in *Appendix X* was included in the customer documentation submitted by Diebold to the TTBR, nor is any mention made in the customer documentation to the existence of such a policy.

In assessing the adequacy and accuracy of security information in both the GEMS TDP and the GEMS customer documentation, many discrepancies surfaced. A great number of security regulations are substantially different as between the two Diebold policy documents. The mandatory policy set forth in

[61] 2002 VSS @ 2.3.2.1 (g).

[62] *GEMS 1.18 TDP Appendix X: Client Security Policy*.

[63] *GEMS 1.18 Technical Data Package: System Functionality Description, Revison 3.0,* p. 2-5.

areas such as user account management, password security, system auditing and physical security is markedly different in *Appendix X* and in the GEMS customer documentation. Generally, the policy in *Appendix X* is quite a bit stricter (and more secure) than that disseminated to the electoral jurisdictions in the GEMS documentation..

This set of discrepancies raises serious concerns. First, the qualification and certification processes are premised on the recommendation of the Independent Testing Authorities who evaluate the systems, including system security. An ITA's findings and recommendations are founded on both its own testing and the information in the Technical Data Package supplied by the vendor. The ITAs' determinations that Diebold's systems met or exceed the security requirements of the VSS are likely be predicated, to a significant degree, on the security policies that they expected to be in place in the counties in which the machines are deployed.

The fact that a different, less stringent set of security policies is contained in the customer documentation makes it possible that the ITAs' conclusions were based on the reasonable but flawed assumption that the *Appendix X* security policy would be reflected in the customer documentation and would be in place when the systems were used. Not only is the *Appendix X* policy absent from the customer documentation Diebold submitted to the TTBR, there is no indication in any of the customer documentation that a different policy was submitted for testing. The following tables present a comparison between the mandatory security policy distributed to customers and that submitted to ITAs.

Tables 6.1 – 6.10 Security Policy Discrepancies

The tables below list the provisions of two election systems security policies created by Diebold for use with its voting systems. The columns on the left show the security policy contained in the documentation Diebold provides to customers, the columns on the right show the mandatory client security policy Diebold submitted for ITA testing as part of the GEMS Technical Data Package.

See also Tables 6.11 – 6.14 for details of the security configuration of the GEMS server provided by Diebold for the TTBR study. Note the variance between the user account, password and auditing policies documented by Diebold in Tables 6.1 – 6.10 and those actually implemented on a delivered system.

Table 6.1 **System Account Policy Discrepancies**

System Accounts	
Diebold Security Policies Distributed to Customers Source: *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, unless otherwise indicated.	**Mandatory Client Security Policy Submitted to ITA** Source: *GEMS 1.18 TDP Appendix X: Client Security Policy*.
System is initially configured with anonymous accounts. All system user IDs and passwords must be maintained in a private and secure manner, conforming with local security requirements.	Every user must have a single unique user-ID and a personal secret password. This user-ID and password will be required for access to multi-user computers and computer networks. Each computer and communication system user-ID must be unique and forever connected solely with the user to whom it was assigned.

The election Security Administrator should be assigned responsibility for the issuance and renewal of user IDs and passwords. Accuvote-TSX: There are three different types of access cards: voter access cards, Supervisor cards, and Central Administrator cards. (*AccuVote-TSX Pollworker's Guide v. 5.0*, page 5-1) Voter access cards are encoded by pollworkers, given to voters, used once, and then returned to the pollworkers. Once a ballot has been cast with a voter access card, the card is deactivated and needs to be re-encoded with ballot information before it can be reused. (*AccuVote-TSX Pollworker's Guide v. 5.0*, page 5-1) Supervisor cards are given to designated pollworkers and used to exit the Official Election screen and access the pollworker functions, such as encoding voter access cards. Supervisor cards are also used to end voting on the AccuVote-TSX unit at the end of an election. (*AccuVote-TSX Pollworker's Guide v. 5.0*, page 5-1) Central Administrator cards can be used by election administrators to access the administrative menu interface. They may also be used in lieu of a pollworker card to access pollworker functions, but it is not recommended that Administrator cards be distributed to pollworkers. Both Supervisor cards and voter access cards are required on election day. (*AccuVote-TSX Pollworker's Guide v. 5.0*, page 5-1) The same Supervisor password must be used for all memory cards in an election, but the password may vary from election to election. (*AccuVote-TSX Pollworker's Guide v. 5.0*, page 5-1)	Without specific written approval from Director of Information Security or equivalent title and authority, administrators must not grant system privileges to any user. User-IDs may be granted to specific users only when approved in advance by the user's immediate supervisor. Prior to being granted to users, business application system privileges must be approved by the involved information owner. The system privileges granted to every user must be reevaluated by the user's immediate manager every six (6) months. This reevaluation involves a determination whether currently-enabled system privileges are still needed to perform the user's current job duties. All user-IDs must automatically have the associated privileges revoked after a thirty (30) day period of inactivity. Management must promptly report all significant changes in end-user duties and/or employment status to the system security administrators handling the user-IDs of the affected persons. So that their privileges may be expediently revoked on short notice, records reflecting all the computer systems on which users have user-IDs must be kept up-to-date. All information systems privileges must be promptly terminated at the time that a worker ceases to provide services to the Diebold Election Systems client jurisdiction. Unless approved by authorized officials at the client jurisdiction and Diebold Election Systems, unauthorized staff and contractors must not enable any trusted host relationships between computers connected to the network containing product servers, workstations, or voting and ballot counting devices. A trusted host relationship involves the sharing of data files or applications across computers, or the elimination of the need to log-into more than one computer.

Table 6.2 **Account Privileges and Access Limitations Policy Discrepancies**

Account Privileges and Access Limitations	
Diebold Security Policies Distributed to Customers Source: *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, unless otherwise indicated.	**Mandatory Client Security Policy Submitted to ITA** Source: *GEMS 1.18 TDP Appendix X: Client Security Policy*.
User IDs and passwords are used to restrict access to software functions to authorized individuals only. Access to user IDs and passwords should be limited to authorized users of the corresponding application only. There are two access security levels in GEMS: • Administrator – may perform any activity in GEMS • Non-Administrator – prevented from changing the election status once the election status has been set to 'Set for Election' and from clearing vote counters Accuvote: A Supervisor card must be entered into the smart card reader, followed by a Supervisor password in order to end the election or access to critical administrative functions on the AccuVote-TS or AccuVote-OS. Access to voter access card encoding devices, such as Voter Card Encoder or VCProgrammer, is restricted to authorized pollworkers only. A single account is used by all pollworkers dialing logging in to the GEMS server to upload memory cards. The smart card key, the data key, and the Supervisor password should be changed across all smart cards-activated devices used in the election. Limit Access to AccuVote-OS Ender Cards Access to the Supervisor card and Supervisor password should be limited to the chief election judge at the polling	Beyond that which they need to do their jobs, computer operations staff must not be given access to—or permitted to modify--production data, production programs, or the operating system. Privileges must be established such that system users are not able to modify production data in an unrestricted manner. Users may only modify production data in predefined ways that preserve or enhance its integrity. In other words, users must be permitted to modify production data ONLY when employing a controlled process approved by management. System privileges must be defined so that non-production staff (internal auditors, information security administrators, programmers, computer operators, etc.) are not permitted to update "production" election system-related information. Special system privileges must be granted only to those who have attended an approved systems administrator training class. The number of privileged user-IDs must be strictly limited to those individuals who absolutely must have such privileges for authorized business purposes. System privileges beyond the capabilities routinely granted to general users must be approved in advance by the Information Security Manager. All software installed on multi-user systems must be regulated by approved access control systems software. This means that a user's session must initially be controlled by approved access control systems software, and if defined permissions then allow it, control will then be passed to separate application software.

locations. Equipped with the Supervisor card and password, the chief election judge has exclusive jurisdiction to end the election on election day.	Multi-user systems administrators must have at least two user-IDs. One of these user-IDs must provide privileged access and be logged; the other must be a normal user-ID for the day-to-day work of an ordinary user.

Table 6.3 **Password Policy Discrepancies**

Password Policies	
Diebold Security Policies Distributed to Customers Source: *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, unless otherwise indicated.	**Mandatory Client Security Policy Submitted to ITA** Source: *GEMS 1.18 TDP Appendix X: Client Security Policy*.
Passwords assigned should be sufficiently difficult to guess so that users are not tempted to impersonate other users. Network and operating system password features usually support mechanisms for preventing the use of trivial passwords Between elections, customers should review all defined users and change all passwords to reduce the exposure to password guessing. All security related data, including security keys, must be maintained confidential at all times.	Passwords must be at least 7 characters. Systems should force users to change their passwords at least every 45 days. On all multi-user machines, system software or locally developed software must be used to maintain an encrypted history of previous fixed passwords. The history file must minimally contain the last ten (10) passwords for each user-ID.
Passwords are set by administrative users which may use a password generator if deemed appropriate.	If passwords or Personal Identification Numbers (PINs) are generated by a computer system, all software and files containing formulas, algorithms, and other specifics of the process must be controlled with the most stringent security measures supported by the involved computer system.

Table 6.4 **Configuration Security Discrepancies**

Configuration Security	
Diebold Security Policies Distributed to Customers Source: *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, unless otherwise indicated.	**Mandatory Client Security Policy Submitted to ITA** Source: *GEMS 1.18 TDP Appendix X: Client Security Policy*.
No software should be installed on the GEMS server or any other PC installed with election management software other than the approved software, as and when authorized, and performed by an authorized official only. No Diebold Election Systems, Inc. software product should be used in a manner other than as intended, that is, in a manner contravening recommended usage procedures provided in Diebold Election Systems, Inc. product support documentation. No alteration of system files should be performed on the GEMS or any other PC installed with election management software, unless explicitly approved by authorized officials, and in an authorized manner only. The versions of all software products used in an election should be verified prior to an election, and verified again prior to critical points in the election management process.	Unless permission of the Director of Information Security has been obtained, the use of direct database access utilities in the production environment is not permitted because these programs will circumvent database synchronization and replication routines, input error checking routines, and other important control measures.

Table 6.6 **Network Connectivity and Security Discrepancies**

Network Connectivity and Security	
Diebold Security Policies Distributed to Customers Source: *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, unless otherwise indicated.	**Mandatory Client Security Policy Submitted to ITA** Source: *GEMS 1.18 TDP Appendix X: Client Security Policy*.
GEMS and GEMS client products operate on a stand-alone basis – and thus are not vulnerable to electronic intrusion – other than: • Downloading AccuVote-TS memory cards • Downloading AccuVote-OS memory cards • Downloading CTS vote centers • Uploading AccuVote-TS memory cards • Uploading AccuVote-OS memory cards • Uploading CTS vote centers • Running AccuVote-OS Central Count At no point are AccuVote-TS units, AccuVote-OS units, or CTS workstations connected to the internet in the course of voting or ballot counting. No wireless communication is enabled or employed between the GEMS server and any of the GEMS client devices. To restrict the possibility of unauthorized access to the GEMS server, modems connected to the server -through which polling location uploads will proceed should be powered on only in the course of upload testing, and following election close. Once all polls have uploaded, modems should be powered off. If the network used for downloading or uploading is physically integrated into a larger network, the components used for downloading should be isolated from the remaining network environment by means of a firewall. Any Election Reporting Client machines to which GEMS issues results (over an IP	The internal system addresses, configurations, and related system design information for networked computer systems must be restricted such that both systems and users outside the internal network cannot access this information. Any computers that can be reached by third-party networks (dial-up lines, value added networks, the Internet, etc.) must be protected by a privilege access control system approved by the client jurisdiction Information Security Department as well as Diebold Election Systems. This policy does not apply to computers which use modems to make outgoing dial-up calls, provided these systems do not receive unattended incoming dial-up calls. Public Internet servers must be placed on subnets separate from internal networks. Routers or firewalls must be employed to restrict traffic from the public servers to internal networks. All inbound dial-up lines connected to internal networks and/or computer systems containing computers should pass through an additional access control point (such as a firewall), which has been approved by the Information Security Department, before users reach a log-in banner. All in-bound real-time external connections to internal networks and/or multi-user computer systems containing servers, workstations, and other electronic devices must pass through an additional access control point (aka a firewall, gateway, or access server) before users can reach a log-in banner. No intranet servers, electronic bulletin boards, local area networks, modem connections must be established with computers without the specific approval of the client jurisdiction and Diebold Election

connection) should be secured within a firewall to prevent potential intrusion, either into the Election Reporting Client machines or the GEMS server. Since any FTP server to which an Election Reporting Client communicates will normally be resident outside of the firewall, unauthorized access to unofficial election results reports should be prevented by maintaining access to the FTP server secure. It will not be possible to access the GEMS database by means of an FTP server to which the Election Reporting Client communicates. The GEMS server is capable of transmitting data to the AccuVote-TS in encrypted format using Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. The purpose of encryption is to prevent the unauthorized interception and interruption of results uploads from the AccuVote-TS units to the GEMS server at election close. SSL/TLS transmission to the AccuVote-OS is not supported. AccuVote-TS memory cards should be programmed over a local area network connecting the GEMS server and AccuVote-TS units in a secure manner, isolated from the external network environment. At no time should memory cards downloaded with election information be left unattended, and should always be under the observation of at least two Chief election judges.	Systems. This policy helps ensure that all networked systems have the controls needed to prevent unauthorized access. Unattended active network ports which connect to the internal computer network must not be allowed in public areas including building lobbies, company cafeterias, and conference rooms readily available to outsiders. The election jurisdiction must maintain a current inventory of all connections between all election servers and workstations to external networks. Cable modems must not be used to connect to any servers and workstations unless a firewall and a virtual private network (VPN) is employed on the involved computers. Dial-up modems should not be connected to servers and workstations which are simultaneously connected to a local area network (LAN) or another internal communication network. No modem lines should be connected to computers or networks, unless these lines have first been approved by the client jurisdiction and Diebold Election Systems. Jurisdiction workers must not establish any communications systems which accept in-coming dial-up calls unless these systems have first been approved by the Director of Information Security. If a computer user attempting to gain access via a dial-up line has not provided a correct password after three (3) consecutive attempts, the connection must be immediately terminated.

Table 6.7 **Logs and Auditing Policy Discrepancies**

Logs and Auditing	
Diebold Security Policies Distributed to Customers Source: *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, unless otherwise indicated.	**Mandatory Client Security Policy Submitted to ITA** Source: *GEMS 1.18 TDP Appendix X: Client Security Policy*.
All activities in GEMS are posted to the Audit Log. It is not possible to delete the Audit Log, or in any way alter it, other than by the automatic posting of an entry for every event to the log. Audit logs are also maintained in the same manner for the AVServer console, in which all AccuVote-TS, AccuVote-OS Precinct Count, and CTS transmission events are logged, Central Count Server console, in which all AccuVote-OS Central Count transmission events are logged Poster, in which all database posting-related events are logged Regional Server/Send Regional Results console, in which all regional transmission events are logged Every transaction on the AccuVote-TS unit is audited. Audit transactions are stored in chronological order, and may not be altered. Every memory card inserted into the AccuVote-TS unit is recorded in the Audit Log. Every memory card upload is recorded on the AVServer console in GEMS – the memory card entry is flagged as uploaded under the Vote Centers tab, while the event is logged under the Log tab. Failure of a transmission between an AccuVote-OS device and the GEMS server will be automatically logged in the GEMS AVServer console log Every transaction on the AccuVote-OS unit is audited. Audit transactions are stored in chronological order, and may not be altered. Every memory card inserted into the AccuVote-OS unit is recorded in the Audit Log. All equipment preparation, testing, and repair activities should be logged once they have been completed. Every programmed AccuVote-TS and	All user-ID creation, deletion, and privilege change activity performed by systems administrators and others with privileged user-IDs must be securely logged and reflected in periodic management reports. All production application systems which handle sensitive information must generate logs that show every addition, modification, and deletion to such sensitive information. Computer systems must securely log all significant security relevant events. Examples of security relevant events include: password guessing attempts, attempts to use privileges that have not been authorized, modifications to production application software, and modifications to system software. Logs of computer security relevant events must provide sufficient data to support comprehensive audits of the effectiveness of, and compliance with security measures. All privileged commands issued by computer system operators must be traceable to specific individuals via the use of comprehensive logs. All computer systems running production servers and workstations should include logs which record, at a minimum the following data: (1) user session activity including user-IDs, log-in date/time, log-out date/time, and applications invoked, (2) changes to critical application system files, (3) additions and changes to the privileges of users, and (4) system start-ups and shut-downs. Log-in passwords must not be recorded in system logs unless these same system logs encrypt the passwords. Computerized logs containing security relevant events must be retained for at

AccuVote-OS should be labeled.

All administrative reports issued in the course of GEMS database development are reviewed, approved, and filed.

Election results reports should be printed and filed once designated voting and Logic and Accuracy testing has been completed prior to election day. These reports confirm that the voting device counts and tallies votes as intended, and may be verified against manual tally sheets prepared for Logic and Accuracy testing process.

The Audit Log is printed and filed once designated voting and Logic and Accuracy testing has been completed prior to election day.

The act of setting memory cards to Election Mode by authorized election staff is logged by the same staff.

Zero Totals reports printed at the outset of voting are signed by authorized election judges, attesting to the fact that all race and candidate counters are zero.

Voters are logged in the pollbook as they are issued voter access cards.

Election Totals reported printed at the conclusion of voting are signed by authorized election judges, attesting to the fact that the voting process proceeded correctly, and that results are present on the Election Totals report.

All voting devices must be accounted for.

All voter access card encoding devices must be accounted for.

All smart cards and election supplies must be accounted for.

All ballots must be accounted for.

All Audit Logs are printed and archived following election close.

PC-based Event Viewer logs should be reviewed and any anomalies accounted for.

Voted memory cards are stored for the obligatory 22 months following the

least three (3) months.

During this period, such logs must be secured such that they cannot be modified, and such that they can be read only by authorized persons. These logs are important for error correction, forensic auditing, security breach investigations, and related efforts.

To assure that users are held accountable for their actions on production computer systems, one or more logs tracing security relevant activities to specific users must be securely maintained for a reasonable period of time.

Application and/or database management system (DBMS) software must keep logs of user activities and statistics related to these activities which will allow them to spot and issue alarms reflecting suspicious business events.

Mechanisms to detect and record significant computer security events must be resistant to attacks.

These attacks include attempts to deactivate, modify, or delete the logging software and/or the logs themselves.

All system and application logs must be maintained in a form that cannot readily be viewed by unauthorized persons. A person is unauthorized if he or she is not a member of the internal audit staff, systems security staff, systems management staff, or if he or she does not clearly have a need for such access to perform regular duties. Unauthorized users must obtain written permission from the Information Technology Manager prior to being granted such access.

To allow proper remedial action, computer operations or information security staff should review records reflecting security relevant events on multi-user machines in a periodic and timely manner.

Users of production servers and workstations should clearly informed which actions constitute security violations. Users must also be informed that such violations will be logged.

A file naming convention must be

election. The GEMS database with final election results is backed up and archive Documenting the *chain of custody*, or flow of materials through the election lifecycle, should allow every significant event pertaining to a critical item in the election to be traced to a specific individual or set of individuals, place, and time. Chain-of-custody procedures pertain to the following critical election equipment: Election servers and clients AccuVote-TS units AccuVote-OS units Memory cards Voter Card Encoder units VCProgrammer units Supervisor cards Voter access cards AccuVote-OS ballots [The *Guide* presents samples of thorough chain of custody forms for use by election jurisdictions to track important events in the lifecycle of the election hardware and supplies.]	employed to clearly distinguish between those files used for production purposes and those files used for testing and/or training purposes. Every multi-user system should include sufficient automated tools to assist the security administrator in verifying the security status of the computer. These tools must include mechanisms for the correction of security problems.

Table 6.8 **Vulnerability Testing Policy Discrepancies**

Vulnerability Testing	
Diebold Security Policies Distributed to Customers Source: *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, unless otherwise indicated.	**Mandatory Client Security Policy Submitted to ITA** Source: *GEMS 1.18 TDP Appendix X: Client Security Policy*.
No attempt is made to perform unauthorized activities with the voting devices. *(sic)*	Workers must not test, or attempt to compromise internal controls unless specifically approved in advance by the client jurisdiction and Diebold Election Systems. Users must not exploit vulnerabilities or deficiencies in information systems security to damage systems or information, to obtain resources beyond those they have been authorized to obtain, to take resources away from other users, or to gain access to other systems for which proper authorization has not been granted. All such vulnerabilities and deficiencies should be promptly reported to the Manager of Information Security.

Table 6.9 **Data Modification Policy Discrepancies**

Data Modification	
Diebold Security Policies Distributed to Customers Source: *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, unless otherwise indicated.	**Mandatory Client Security Policy Submitted to ITA** Source: *GEMS 1.18 TDP Appendix X: Client Security Policy*.
GEMS database development should proceed according to authorized election development policy only.	Privileges must be established such that system users are not able to modify production data in an unrestricted manner. Users may only modify production data in pre\defined ways that preserve or enhance its integrity. In other words, users must be permitted to modify production data ONLY when employing a controlled process approved by management. Updates to production databases must only be made through established channels which have been approved by management.

Table 6.10 **Physical Security Policy Discrepancies**

Physical Security	
Diebold Security Policies Distributed to Customers Source: *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, unless otherwise indicated.	**Mandatory Client Security Policy Submitted to ITA** Source: *GEMS 1.18 TDP Appendix X: Client Security Policy*.
AccuVote-OS firmware is locked inside the AccuVote-OS unit, and should only be accessible to authorized officials. The memory card slot is provided with a cover plate. When this plate is in the closed position, it allows for a security seal to be placed in a hole in the post that the plate fits over. If there is any tampering with the memory card once it is behind this sealed cover plate, the tampering will be evident. Every compartment on a ballot box that is full and has been set aside in the course of voting remains locked, and a security plate locked into the ballot entry slot on the ballot box lid Limit access to voting machine keys. Access to voting equipment, in the warehouse or elsewhere, should be monitored and logged. Voting equipment should be stored according to designated storage conditions only. All security-related supplies, such as Supervisor cards, must be maintained secure at all times. Following the Logic and Accuracy Test, memory cards are locked and sealed into the AccuVote-TS unit, preventing any unrecorded, unauthorized access to the memory card. Access to ballot box and voting device keys is restricted to authorized pollworkers only. The PCMCIA memory card representing primary election storage remains locked and sealed in the election data compartment in the course of voting. Privacy panels on all AccuVote-TS	All clients and employees will receive this and all other related information security policies. Advertising an area as secure should be minimized to decrease notification of a secure area to an unauthorized/malicious party. Structural protection should be maximized within the boundaries outlined within risk assessment. Structural protection applies to all structures housing election equipment, such as a room where election equipment and servers are housed. Secure rooms should be constructed with full height walls. Secure rooms should be constructed with fireproof ceilings. External access to secure rooms should be kept to the least number of privileged personnel. Secure rooms should contain a minimum number of solid, fireproof, and lockable doors required to maintain day-to-day operational efficiency. All points of entry/exit should be observable by authorized security staff. All points of entry/exit in a secure room should have auto-closing devices and/or should never be left open. Any aperture within a point of entry/exit in a secure room such as a window should be reasonably small and provide for a locking mechanism. A procedure should be put in place that allows for maintenance of appropriate locks. All points of entry/exit should remain locked when not in use in coordination with local fire policy. In the case of a breach, all locking mechanisms affected by the method of invasion should be

units are in an open position. Voting equipment is supervised by election judges in the course of election day. No one accesses voting booths other than voters that have been issued voter access cards. Full AccuVote-OS ballot boxes should be sealed. Voters do not leave the polling location with unauthorized materials. Voters do not leave the polling location with ballots or voter access cards. No unauthorized materials are present in or on the voting devices. The grounds of polling locations are maintained secure. No voter access cards are present in the voting area, other than those being held by valid voters. No unauthorized individuals are present at the voting location following election close. Once Voter Card Encoder units have been encoded, they should be stored in sealed, secure containers, and the seal numbers recorded. It is essential that all election facilities be maintained in a secure manner at all times, for the entire duration of the election equipment in the facilities, in the course of the election lifecycle, and beyond. Access to facilities containing election equipment should be limited to authorized election staff only. Every access to facilities containing election equipment should be documented. A sign-out sheet should be completed for every item of election equipment removed from or returned to the warehouse, including the device name, serial number, sign-out time, name and signature of the official signing out equipment, and the return time as well	changed. The method/device used to change the locking mechanism should effectively remedy the invasion tactic used by the unauthorized third party. Alternative physical security strategies should be periodically investigated and considered by the security staff. Where applicable, the use of secondary window restraint devices (e.g. window bars) should be considered. Where applicable, the use of anti-theft cabling with centralized alarm monitoring should be considered. Such scenarios would include, but not be limited to, any device containing, processing, or interacting with data/processes classified as PRIVATE or higher. The use of a more robust locking mechanism on all points of entry/exit should be considered. The system should include centralized monitoring of all door events and provide for two-factor authentication if possible (e.g. magnetic key cards, proximity cards, biometrics). The above said events provided by the system should be able to be categorized by the security staff and acted upon by a third party alarm/notification system. The use of a monitored alarm system in the secure room should be considered. The alarm system should provide for unauthorized entry notification and detected motion notification when activated. The service should be monitored by a third party security service if in-house security staff does not have the resources to monitor the system 24/7. The use of a monitored video surveillance system in the secure room should be considered to provide visual confirmation of an act of malice. The system should provide coverage of all points of entry/exit and all assets within the secure room classified as PRIVATE or higher. The coverage should be

as name and signature of official returning equipment. All facilities should be characterized by the following: Access limited to authorized individuals only Approved screening process for determining election official authorizations Proven tools and services to secure facilities, including: Physical door and window locks Electronic door and window locks, including: Password-based access Smart card-based access Biometric-based access Security guards Since voting devices, memory cards, AccuVote-OS ballots, and voter access card devices are normally warehoused separately from the election administration office, the destruction of the election administration office should affect the GEMS server, server communication devices, such as modems, and possible archive materials only.	configured in such a manner that a visual confirmation of an individual's profile and unmistakable facial/body characteristics can be attained. All video should be retained for the period of time needed to review by an authorized security personnel. The system should provide for a method to remove the video from the recording device onto another media for transportation or archival in the case of an incident being recorded. Proper disposal of confidential waste should be carried out in a careful and adequate manner to maintain confidentiality. A documented procedure should be distributed to all associates whose roles and responsibilities outline their handling of confidential material. This procedure should document in detail the use of a company provided facility that will properly and thoroughly destroy (e.g. using an industrial shredding device) the material. The documented procedure should also properly describe the destruction of materials based on their associated retention policy. Business critical systems should be separated from general systems. To prevent covert use, workstations not routinely used to display sensitive information should be stored in open, visible spaces. Maintain a secure inventory of all equipment and peripheral equipment, with up-to-date logs of manufacturers, models, and serial numbers. Consideration should be given to the use of videotape for insurance purposes. All mobile computing devices, such as laptops, should be locked in a secure cabinet while not in use. All computers should be logged off when the operator is not in the vicinity of the computer. Use a managed virus scanner on all

	computers at all times. A regular schedule for updates to the virus scanning engine should be documented and performed according to the virus scanner creator’s virus profile release cycle. A regular schedule for full local and network virus scanning should be documented and performed. All third party computers that need to participate on your network should be inspected and virus scanned by a security staff before being connected. All peripheral devices should be distributed and implemented based on user’s privilege level. A documented usage outline should be completed by authorized security personnel for every device used for day to day operations. A method should be devised to allow for centralized monitoring of problem detection on all devices. Equipment labeling should be created and implemented in covert and overt ways as to make unauthorized tampering more difficult.

Given the very short span of time for the Documentation Team’s review of the TDP containing the Client Security Policy discussed above, it is not possible to conclude whether the security practices described in the Client Security Policy can be successfully and practically implemented in the use of Diebold voting systems.

6.2 Treatment of Security Issues in the Customer Documentation

The product documentation that Diebold distributes has significant information about the security features of its systems and, to a degree, how best to conduct election tasks in a way that leverages security features built in to the system. Election administrators can read the documentation to find out about some security hazards and prudent precautions. The documentation also includes useful sample forms for tracking the chain-of-custody of voting equipment and supplies. Some aspects of the documentation related to security, however, are cause for concern.

The documentation of security issues that is provided to the customers does not adequately explain the threats that the Diebold policies are designed to address. The coverage of security topics is generally limited to broad statements that certain threats are not realistic or that the recommended safeguards eliminate entirely the threats that they are designed to address. At many places in the customer documentation, the treatment of security issues amounts to categorical statements that the system is not vulnerable to a certain threat, and thus vigilance in that area is unnecessary. For example: “No system functionality is accessible by connecting an external electronic device to an AccuVote-TS port, and no port is physically accessible when the Accu-Vote TSx is configured for voting on election day."[64] This comment suggests that no vigilance is warranted in the face of someone, perhaps a voter, connecting an external electronic device to a port on a voting machine. The comment also tends to suggest that the reader accept the inviolability of the rather flimsy lock and plastic door that guard the port compartments.

Similarly problematic are passages such as:

> GEMS and GEMS client products operate on a stand-alone basis – and thus are not vulnerable to electronic intrusion – other than:
>
> - Downloading AccuVote-TS memory cards
> - Downloading AccuVote-OS memory cards
> - Downloading CTS vote centers
> - Uploading AccuVote-TS memory cards
> - Uploading AccuVote-OS memory cards
> - Uploading CTS vote centers
> - Running AccuVote-OS Central Count[65]

Here, the documentation offers a brief list of possibly vulnerable operations that purports to be exhaustive. The ever expanding breadth of known techniques for electronic intrusion, the degree of interaction with the devices by members of the public and pollworkers, and the paucity of reliable detection capabilities renders this statement not only false but perhaps detrimental to achieving and safeguarding the system's security. It suggests that outside of these seven enumerated windows of vulnerability, no vigilance is needed.

In short, such reassurances do not seem to advance any security objective, but rather to impress the reader with the security of the voting device and reduce his vigilance. Similarly, comments such as "uploading a memory card provides no ability to alter the contents of the memory card,"[66] even if true, do not advance security so much as reassure the reader.

Persistently, the manuals do not explain the risks to be avoided by specific security policies. Thus, officials have no means of evaluating Diebold's proposed security policies. They cannot adapt policies to unique jurisdictional needs, applicable regulations, available resources, or otherwise make decisions about security policies independent from the vendor. The categorical dismissal of threats, coupled with a lack of information about the actual behavior of the voting systems in relevant contexts, both discourage independent assessments of security matters and deprive officials of the information required to undertake such assessments.

The potential harm caused by the promulgation of questionable or ill-suited security procedures is compounded by documentation statements including: "No Diebold Election Systems, Inc. software product should be used in a manner other than as intended, that is, in a manner contravening recommended usage procedures provided in Diebold Election Systems, Inc. product support documentation."[67]

[64] *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, p. 16-4. Statement is repeated in reference to the AccuVote-OS on page 16-7.

[65] *GEMS 1.18 Election Administrator's Guide, Revision 8.0,* p. 16-13.

[66] *GEMS 1.18 Election Administrator's Guide, Revision 8.0,* p. 16-5.

[67] *GEMS 1.18 Election Administrator's Guide, Revision 8.0,* p. 16-12.

The customer documentation discussion of security issues also tends to mischaracterize or overstate the protection provided by certain safeguards. There are instances throughout the documentation in which tamper-evident seals are said to "prevent tampering."[68] Similarly, the use of encryption is said to prevent disruption of communications.[69] Though the voting devices' plastic doors with small barrel-key locks are easily bypassed, the doors are presented as effective in blocking access to the compartments inside. There are instances in which passages in the documentation are not merely unhelpful, but could potentially lead to overconfidence in the face of a potential threat, such as:

> Once the Logic and Accuracy Test is complete, memory cards are sealed into voting machines, a numbered seal is placed on the PCMCIA compartment door as well as the enclosing voting booth of all AccuVote-TS units, as well as over the memory card slot of all AccuVote-OS units, and the seal numbers recorded by election officials in order to prevent tampering of *(sic)* the units.[70]

6.3 Security Configuration of the GEMS Server Provided to the TTBR

As described in Section 4.3, we performed a configuration audit of the GEMS server that was provided to the TTBR red team testing room at the SOS facility in Sacramento. We were informed by Diebold technical personnel that the GEMS server was configured just as one would be when delivered to an election jurisdiction in California. Part of the configuration audit focused on the security settings on the TTBR server.

Among the security-related findings of our configuration audit was that none of the user account and password policies were active on the GEMS server. (See Section 6.1 for a discussion of password policies in the Diebold documentation.) Password policies such as minimum length, strength requirements, and history retention were not implemented.

We also found that none of the system-level auditing of security events was enabled, despite the fact that the GEMS configuration described in the *GEMS 1.18 Server Administrator's Guide* states that the security logging should be enabled and verified to be active. Our examination of other operating-system audit logs found that the Windows Application log, System log and Security log were all configured to retain records of events for only 7 days and that the logs were limited to 512 KB in size. Maintaining all logs of election audit information for a minimum time period (far greater than 7 days) is a requirement for election security audits and other examinations, as well as federal law. Care should be taken to make sure that California counties that have received GEMS servers configured by Diebold are not being placed in violation of federal or California law due to improperly configured logs on their GEMS servers.

It should be noted that, while it is advisable for election officials to configure security settings on systems in a manner consistent with approved security policies, the GEMS configuration documentation that is provided to customers does not describe the procedure for effecting the proper security settings. The customer documentation's sole mention of such settings is in the *GEMS 1.18 System Administrator's Guide*, which describes a process to view the logs[71] but none to configure them properly. An industrious election official may undertake to fix relevant settings upon viewing that the settings were not correct, but

[68] For examples, see *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, p. 2-6 and p. 4-133.

[69] *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, p. 16-12.

[70] *GEMS 1.18 Election Administrator's Guide, Revision 8.0*, p. 2-6.

[71] The document directs the reader to the Windows Event Viewer and instructs, "[c]lick on the Security entry in the left-hand display panel, and observe the system related events that appear in reverse chronological order in the right-hand display panel." *GEMS 1.18 System Administrator's Guide, Revision 6.0*, p. 3-8.

would do so with no help from the Diebold documentation. The only document that offers any significant coverage of platform security configuration is the *GEMS 1.18 Server Administrator's Guide*, which is not to be circulated outside of Diebold.[72]

The following two tables present the system security related findings of our configuration audit of the GEMS server provided to the TTBR study.

Table 6.11 **Selected Security Settings on the TTBR GEMS Server**

Selected Security Settings	
Policy	**Effective Setting**
Audit access of global system objects	Disabled
Audit use of backup and restore privilege	Enabled
Allow system to be shut down without having to log on	Disabled
Automatically log off users when logon time expires	Enabled
Digitally sign client communication	When possible
Digitally sign server communication	Disabled
Disable CTRL+ALT+DEL requirement for logon	Enabled
Do not display last user name in logon screen	Enabled
Prevent system maintenance of computer account password	Disabled
Recovery console: allow automatic administrative logon	Disabled
Recovery console: allow floppy access to all drives and all folders	Disabled

Table 6.12 **Password Policies on the TTBR GEMS Server**

Passwords	
Enforce password history	0 passwords remembered
Maximum password age	42 days
Prompt user to change password before expiration	14 days
Minimum password age	0 days
Minimum password length	0 characters
Passwords must meet complexity requirements	Disabled
Account lockout duration	Not defined
Account lockout threshold	0 invalid logon attempts
Reset account lockout counter after	Not defined

[72] "The *GEMS 1.18 Server Administration Guide* is intended for technical support staff internal to Diebold Election Systems, Inc. only. It is not intended for use external to Diebold Election Systems, Inc. The document provides a detailed framework for the configuration of GEMS servers." *GEMS 1.18 Server Administration Guide, Revision 3.0,* p. 1-1.

Table 6.13 **Event Logging Settings on the TTBR GEMS Server**

Event Logging	
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing
Application Log - Maximum log size	512 KB
Application Log - Overwrite events older than	7 days
Security Log - Maximum log size	512 KB
Security Log - Overwrite events older than	7 days
System Log - Maximum log size	512 KB
System Log - Overwrite events older than	7 days

Table 6.14 **Possibly Unneeded Services on the TTBR GEMS Server**

Possibly Unneeded Services	
Service	**Start Setting**
NetMeeting Remote Desktop	Manual
Remote Registry Service	Manual
Telephony	Manual (was running at the time of configuration audit)
Telnet	Manual
Windows Installer	Manual
Wireless Configuration	Manual

Conclusion: Vendor Nonconformity Responses

The Diebold documentation is incomplete and faulty in certain ways. The Source Code and Red Teams have identified some major vulnerabilities with key components of the Diebold VS.

In addressing Diebold voting systems' areas of potential nonconformity with applicable standards, regulations and conditions of certification, election officials may wish to be aware of the Diebold corporate policy to nonconforming products. In case remediation is sought, the following policy might be useful:

From the **Diebold North America: Quality Systems Manual** QSM00001 Version 15.0 ["QSM"]

In the "Control of Nonconforming Product" material, the QSM states that "Diebold ensures" that any "product which does not conform to product requirements" will be "identified and controlled to prevent its unintended use or delivery." The manual directs further consultation for "controls and related responsibilities and authorities" to QSP00013, Control of Nonconforming Product.

The QSM represents that "nature of nonconformities and any subsequent actions taken, including concessions obtained" are the subject of company records. It further warrants that if a "nonconforming product is detected after delivery or use has started," Diebold will undertake "action appropriate to the effects, or potential effects" of the product's failure to confirm.

Other Diebold North America Manuals relevant to dealing with nonconforming products include QSI00025, Global Manufacturing Customer Relations Process and QSI00002, Field Change Order (FCO) Process.

If the California SOS identifies any material deficiencies or departures from the operative product requirements, these manuals' policies may prove relevant. [73]

[73] Section 6.1 of this Documentation Report contrasts the mandatory client security policy ("Appendix X") that was part of the vendor's confidential submission to CIBER for Federal ITA qualification testing with the security policies set forth in the documentation provided to customers, pointing out areas in which they significantly differ or conflict. Appendix X mandates election jurisdiction security policies and practices that are significantly stricter.

On August 24, 2007, the Cal-SOS informed us that it had just learned that, in possible contrast to the vendor documentation this team was provided for the TTBR evaluation, the vendor has stated that it has made available to California counties a Client Security Policy (CSP) document. The vendor (formerly Diebold, now Premier Election Solutions, Inc.) stated that beginning in 2004 as part of a legal settlement, it has provided, upon request, a CSP document to California counties that have purchased its election systems. The vendor further stated that a CSP document has been included on product documentation CDs beginning sometime in 2006.

The CSP that the vendor states has been disseminated to California counties is not referenced in any of the documents that were provided for the TTBR, nor was the team provided a copy of this CSP document to review. We are thus unable to determine whether the CSP reflects precisely the mandatory security policies that the vendor submitted for its system's certification and qualification reviews, or compare it to the vendor's other security policy documentation. *[Added to the original Report on August 27, 2007]*