

Bruce McDannold
Election Systems Division
Office of the Secretary of State
1500 11th Street
Sacramento CA 95814

11 Nov 2005

Subject: 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.

Executive Summary

The Diebold Election Systems, Inc. (DESI), Voting System requested certification of:
GEMS Software version 1.18.24
AccuVote-TouchScreen-x (AV-TSx) with AccuView Printer Module (AVPM), Firmware
3.0.3
AccuVote-TSX Ballot Station firmware version 4.6.4
AccuVote-Optical Scan (AV-OS) (model D) with firmware version 1.96.6
AccuVote-Optical Scan Central Count (AV-OSCC) firmware version 2.0.12 with
AccuFeed
Voter Card Encoder (Spyrus) version 1.3.2
Key Card Tool software version 4.6.1
VoterCard Programmer (VCProgrammer) software version 4.6.1

We conducted certification testing in Sacramento, CA in June 2005, Stockton, CA, in July 2005, and finally at the Bahai Hotel San Diego 26-29 September 2005.

The AV-TSx was decertified in April 2004 with a condition that recertification would require the addition of an Accessible Voter Verified Paper Audit Trail (AVVPAT) capability. The San Diego test was the finale of a series of tests to qualify the AV-TSx with AVPM, DESI's implementation of the AVVPAT requirement. Due to problems which occurred in the earlier tests, a requirement was added to perform Volume testing of the DREs. Results from the volume testing led to a series of improvements to the AVPM units and AV-TSX Ballot Station firmware. [See the Staff Review and Analysis for a detailed report on these tests

The testing included the DESI procedures [Services] submitted to satisfy Paragraph 6.3.y of Superior Court Case No. RG03 128466. The test confirmed that the Windows secure setup proposed permitted full operation of GEMS in a more secure mode. Two services which were expected to be stopped by the changes were not successfully stopped; DESI needs to provide a further revision to the procedures to complete the requirement.

I received source code files for ABasic Report file 195US.abo, version 1.15 on 10 Nov 2005 under proprietary information conditions. The preliminary scan and review of the source code files found the given program harmless in its current form. The ITA test reports [Cyber-Add and AVTSx 4.6.4] only tested with 195US.abo. The remaining 23 Report files installed with GEMS 1.18.24 have not been validated for use.

Other significant changes which were successfully exercised in this test are:

- a. Correction of earlier problems which should now permit Provisional ballots to be cast on the AV-TSx.
- b. Correction of minor cast ballot report errors.
- c. Correction in the export operation for an error which resulted in a fatal error preventing exporting of results for some CalVoter submissions.
- c. Addition of security audit logs on the VCProgrammer.
- d. Stronger encryption and PINs for Voter Access cards.

e. Addition of an Administrator card to access critical options in the AV-TSx and to reduce the Supervisor card access to functions needed at the polling place. The change provides separate PINs to be assigned to the two cards.

The AV-TS R6, an earlier DRE model which is certified in California under an earlier version of GEMS, was not included in this certification test.

As configured and presented for testing, this version meets current standards for use in California with the recommendations noted below in the body of the report.

References:

1. [SVF0515] Freeman, *Certification Test for the Diebold Election Systems, Inc. (DESI) GEMS 1.18.22/AV-TSX 4.6.1 Voting System Including the AccuView Printer Module*, 15 May 2005
2. [SOSPROC] Diebold Election Systems, Inc., *State of California PROCEDURES Required for Use of the Diebold Election Systems AccuVote-TSx Electronic Ballot Station [Draft]*, 28 Mar 2005. (More recent draft procedures have been submitted but came in too late to be included in this report.)
3. [Ciber-Org] Ciber Report, *Software Functional Test Report Diebold Election System GEMS 1-18-24, Original Report Version 1.0 created 8/03/05*, .3 Aug 2005
4. [Ciber-Add] Ciber Draft Report, *Software Functional Test Report Diebold Election System GEMS 1-18-24, Addendum 1 for GEMS 1-18-24 created 9/30/05*, changed 11/4/05.
5. [AVTSX-4.6.2] Wyle Report No. 48619-06, *Hardware Qualification Testing of the Diebold Election Systems AccuVote-TSx DRE Voting Machine With AccuView Printer Module (Firmware Release 4.6.21)*, May 17, 2005.
6. [AVTSX-4.6.3] Wyle Report No. 52501-01, *Change Release Report of the Diebold Election Systems AccuVote-TSx DRE Voting Machine With AccuView Printer Module (Firmware Release 4.6.3)*, November 2, 2005
7. [AVTSX-4.6.4] Wyle Preliminary Report No. 52501-01, *Preliminary Change Release Report of the Diebold Election Systems AccuVote-TSx DRE Voting Machine With AccuView Printer Module (Firmware Release 4.6.4)*, November 2, 2005
8. [Services] Diebold Draft Instructions, *Instructions for Setting GEMS and EMP Server Configuration Pursuant to Paragraph 6.3.y of Superior Court Case No. RG03 128466*, 1 Aug 2005.
9. [Admin] DESI Manual, *GEMS_1.18_Election_Administrators_Guide_Revision_9.0*,

Introduction

In compliance with California Elections Code 19200 and 19205, Diebold Election Systems applied for certification for the following

1. GEMS, Version Release 1.18.24
2. AV-TSx R7 running Microsoft Windows CE R7-410.2.1 with AccuView Printer Module.
3. Ballot Station Firmware Release 4.6.4. This firmware is used on the AV-TSx with the AVPM.
4. Key Card Tool Version 4.6.1
5. Voter Card Encoder (VCE) Version 1.3.2
6. VC Programmer Version 4.6.1
7. AV-OS Precinct Firmware Release 1.96.6
8. AV-OS Central Count 2.0.12 Firmware Release 2.0.12

Although not part of the application, the following should be part of the final list:

9. ABasic Report File 195US.abo, Revision 1.15
10. AccuView Printer Module, Firmware

This testing has extended over months to encompass two version changes to GEMS (1.18.22 and 1.18.24), the introduction and further development of the AccuView Printer Module to the AV-TSx with changes in Ballot Station Firmware from 4.6.1 to 4.6.4, minor upgrades to the paper ballot based AV-OS precinct counter, and a significant upgrade to the encryption tools used to identify voter access using the Voter Access Cards. Two new devices, the Election Media Processor and the Express Poll 2000/4000, were introduced during this period but removed from testing pending further developments.

The principle change was the introduction of the AVPM, which supports the requirement for an Accessible Voter Verified Paper Audit Trail (AVVPAT). The AVPM is a modification to the native report printer in the AV-TSX. The new module mounts over the previous report printer unit and provides a second roll of printer paper, which feeds past a view port where the voter can review the printed record of their ballot choices. If the voter accepts the printed version, the ballot is drawn into a secure take-up canister and an electronic image of the ballot is stored in internal memory and a removable memory card along with updating the tally of votes. If the voter rejects the printed audit copy list of choices, the audit record is marked as rejected and is also drawn up into the secure canister but no ballot image is stored and the votes are not added to the tally. The VVPAT canister is sealed before the polls are opened and are removed sealed at the end of the election until the VVPAT records are needed to perform an audit.

During earlier testing of the AVPM, the system had frequent problems with paper jamming and misfeeding of the printer paper. Less than one percent resulted in the VVPAT record being over written, lines lost, or otherwise damaged so the record could not be read or recovered but this was appearing on nearly every AV-TSx submitted for testing. Although an alert voter should note the problem, there was no warning to the voter; inattentive or blind voters could fail to notice a jam that, in testing, resulted in multiple ballots being affected. Improvements to the AVPM operation reduced the frequency of jams and provided controls to prevent the records from being damaged or backed up for multiple voters when jams did occur. During the San Diego volume testing, approximately 10,000 ballots were cast with only three paper jams and two misprints. Only one jam resulted in the paper record being damaged and that error was detected, reported as a printer malfunction, and allowed the voter to cancel the ballot to complete a successful vote. Further details are provided in the Staff Review and Analysis.

In prior certified versions of GEMS, problems with processing provisional ballots required a restriction to not allow the DRE to be used for provisional ballots. GEMS 1.18.24 includes corrections for the invalid reporting of write-ins and allows the ballot image of an accepted provisional ballot cast on an AV-TSx to be printed out in the paper ballot format for transcribing to a paper ballot of the correct precinct.

The AV-TSx supports multiple languages and was tested with seven of California's required languages during ITA testing and with English, Spanish, and Chinese in the latest state testing (earlier tests in this sequence of tests used Vietnamese instead of Chinese). Testing verified the capability to present the ballots in the given language on the screen and on the AVPM record. The AV-TSx was also tested in audio mode supporting HAVA requirements in all languages to confirm every contest, choice, and instruction could be provided and adequate access was supported to allow preview, selection, back-tracking, correction, summary review, and alerting of under-voted and unvoted contests.

The Key Card Tool and AV-TSx Ballot Station firmware now support two levels of administrative access, stronger PINs and encryption keys, and better encryption support. The older Supervisor card is restricted to common poll-worker access functions during poll

operations with the new Administrator card providing controlled access to election official functions which can be restricted to fewer officials. The VC Programmer includes an audit log which permits reviewing the history of cards generated.

DESI provided procedures, in compliance to the Superior Court settlement requirement Paragraph 6.3.y of Superior Court Case No. RG03 128466, to setup the Windows operating system in a more secure operating mode. Prior to the settlement decision, implementation of earlier recommendations resulted in GEMS not always working successfully with the consequence that jurisdictions had to drop back to less secure setups to complete elections. This set of procedures was tested and redefined to confirm full operations of GEMS allowing more aggressively secure election operations and should be incorporated by reference or full text in the California Use Procedures. Two items of the procedure failed to work as expected and need further work before this requirement is considered completed.

The Federal ITA testing of GEMS 1.18.24, AV-TSx 4.6.4, and AV-OS Precinct Ballot Counter 1.96.6 only verified use of the ABasic Report file, 195US.abo, Revision 1.15. The prior California certified versions included a different version of this file and 194US.abo. I preformed a preliminary review and comparison of source code for this revision (a fuller report is being prepared under separate cover) and found that, as installed, version 1.15 does not present any risk to the election reports and makes no changes to recorded votes. The other ABasic Report files remain unverified.

NASED Qualifications/State Certifications

<u>Component</u>	<u>NASED #</u>	<u>State Certification</u>
1. GEMS 1.18.24	N-1-06-22-22-002	none
2. AV-TSx R7 with VVPAT)	N-1-06-22-22-002	none (decertified w/o
a. BS 4.6.4		
b. *AVPM 3.0.3		
3. Key Card Tool 4.6.1	N-1-06-22-22-002	none
4. VCE 1.3.2 (Spyrus)	N-1-06-12-12-002	(1.18.19) 08/10/2004
5. VCE 1.3.2 (Spyrus)	N-1-06-22-22-002	(1.18.24) none
6. VC Programmer 4.6.1	N-1-06-22-22-001	none
7. AV-OS Precinct 1.96.6	N-1-06-22-22-001	none
8. AV-OS CC 2.0.12	N-1-06-12-12-004	(1.18.19) 09/28/2004
	N--1-06-22-22-001	(1.18.24) none

GEMS 1.18.24 and most of the components are qualified under a NASED number in conjunction with BS Firmware 4.6.3 but BS Firmware 4.6.3 did not perform adequately in earlier CA certification testing. Two of the components were previously certified under GEMS 1.18.19 in California but are re-qualified with 1.18.24. The new NASED number was issued 11/10/05 for these components with BS Firmware 4.6.4. Final test reports for this release version have not been received from either the hardware or the software ITAs.

*AVPM unit revision was not recognized in the hardware or software ITA testing. Discussions with the hardware ITA indicate that the modification was probably tested but does not appear to have been included in the documentation to the hardware ITA as a different model. This revision of the AVPM is critical to this test and certification and needs to be recognized in the final certification.

Observations and Issues

(Underlined statements are issues or recommendations that may require further action. Most of these are issues that need to be addressed in the California Use Procedures, which currently are still in draft and changing.)

1. AVPM Model. During the testing, we saw three different versions of the AVPM. There is no external label identifying which version of the AVPM is installed but a report item in the Build Information screen of the AV-TSx lists a firmware revision number. Also, a paper label giving the firmware number may be found under the paper tape source roll inside the AVPM. Checking the AVPM firmware version needs to be included in acceptance testing.
2. Printing and storing zero-total reports and summary/audit reports. The operating procedures require the zero totals report and the reports printed after polls closed to be done with the cover up to allow the report to check and certified by the poll worker. These reports print out without being automatically taken into the security canister. After the reports are certified, the supervisor poll-worker should finish taking up the report so the certified report is stored in the secure canister. In addition to the summary results, I recommend a copy of the audit report also be printed and stored in the secure canister before the canister is removed. An additional copy of the summary results, which may be required, can be printed afterwards and posted locally.
3. Full canisters. We also noticed some hesitation and stopping on the take-up action when the canister came neared to being full. The supply reel provided more paper than fits in the security canister (the take up reel is not as tightly wound as the supply reel). The final test included observations of a low paper check, which appears to adequately prevent a full canister condition. No action required at this time.
4. Magnifying lens. From the [SVF0515] report “The magnifying lens may not be practical for users requiring its use. The limited focused field of view in the paper view window left edges and top/bottom elements in the paper view window distorted. Overhead and side lighting created areas of glare and shadow adding to the potentially difficulty for reading the ballot. The magnification level appeared to meet current expectation for the degree of magnification but we do not have a basis for accepting or rejecting the adequacy of this feature except public comment.” In the final test, DESI has removed the magnifying lens. This may limit the utility of the VVPAT record for some voters with limited visual disabilities who will not be able to read the small AVPM print. The current suggestion is that commercial full page magnifying sheets may be used, but this was not tested. It is not clear whether the magnifying sheets are to be provided as part of the DESI contracts or at the direct expense of the jurisdiction.
5. Blind vs. AVPM. Those voters who are blind or so limited in vision that they cannot read the AVPM record essentially cast their ballot without further verification after the audio summary is reviewed. There is no capability to independently read the AVPPM audit record for blind voters. (See special comment on HAVA requirement.)
6. Physically Disabled. There are no separate features supporting physically disabled voters other than the ability to remove the screen from the voting booth configuration and bringing it closer to the voter in different orientations. In this mode, the AVPM is disconnected and no AVVPAT records will be available for audit. DESI has proposed that physically disabled voters may use mouth-sticks, taking advantage of the touch-screen sensitivity. I recommend that this option, should it be acceptable as satisfying accessibility requirement for disabled voters, be tested with the assistance of actual disabled voters who use such assistive devices; the test involves issues of the positioning of the screen (with implications for the AVVPAT record), distance, and force of contact for which I do not have enough information to set up a valid test. (See special comment on HAVA requirements.)
7. Barcodes. In the original submission of the AVPM, the paper audit record carried a unique identifier which appeared to violate the California Election Code, Chapter 3,

Semifinal Official Canvass, Section 15208. A paper ballot with type of marking would be required to be declared void and ineligible for counting. The same unique identifier could also be used to retrieve and print out the electronic ballot image as the same number was assigned to match it. The identifier was included in a barcode that was imprinted at the end of every cast ballot (rejected ballots contained just a mark labeling them as rejected.) DESI was asked to remove the ballot id and barcode from the AVPM printout to satisfy the Section 15208 requirement. They did so, but left the barcode an optional feature which could be turned on in GEMS. I recommend that a restriction on using the barcode in official elections be included in the California Use Procedures, although there may be some advantages in using the barcode during system testing.

8. Administrator's Card. The new Ballot Station Version 4.6.x firmware includes a requirement for a Central Administrator access card, larger PIN numbers and encryption keys, and a special mode of operation limited to the Administrator access. The Administrator mode supports pre-election setup and diagnostics and post-election maintenance including the capability to work with the secured archives. Some of the more sensitive operations are also available in the Election mode of operation using the Administrator's access card and secure pin. The improved features require Version 4.6.1 of the Key Card Tool to support setting the encryption key and pin number for the Administrator's access card and allows the Administrator's card to be set within the jurisdiction. (In a prior test, the new cards had to be set at a plant in Texas). In the draft use procedures [SOSPROC], the recommendation is that only a few (minimum required is two) Administrator cards be prepared and not distributed to the polling places. (NOTE: Added underline to recommendation)
9. Paragraph 6.3.y of Superior Court Case No. RG03 128466. DESI provided a draft [Services] of the server setup procedures required by Superior Court settlement. The procedures included:
 - Changing services in Windows to reduce the active services to required services only. The procedures went beyond the required shutdown of unneeded *network* services to include other services which were not needed.
 - Issuing legal notices and warning prior to system logon.
 - Setting local machine Windows Security Policies to a minimum security posture.
 - Disabling AutoRun.
 - Hardening the Boot Sequence including passwording the BIOS setup.

When we tested the use of GEMS under this configuration, all changes worked effectively except the stopping of Remote Access Connection Manager and Telephony. Investigating, we determined that the Microsoft default startup was restarting these automatically and a script to edit the Windows Registry was needed to terminate the automatic start. DESI needs to provide the final modification and a test should be conducted to confirm the final setup procedures against this requirement.

For information only. Local jurisdictions are responsible for their own network and information systems security setup and management. Voting system vendors have traditionally not provided direction and have no control over the local security management actions. However, when stronger practices have been attempted by local Information System managers (and even proposed by the vendor), the voting system may become inoperable resulting in better security practices being backed out in the interest of supporting the election resulting in lesser security. This procedure is targeted at providing the local information managers the information so they can recognize what can and cannot be done with out disabling the election operation.

10. User Accounts. The use procedures [SOSPROC] recommend the setup of administrator and user system logons, which allow the restriction to changes to program installations and security settings to a limited set of administrators but permit other authorized workers to access and perform Basic functions in GEMS. In the setup we created accounts for an Administrator and SuperUser but also found we needed a account user group for Nero Burning rights to be able to make CD backups of the election and the election results. In the [Services] procedures, the instructions included setting up machine Security Policies but stopped short of providing instructions for setting Windows Policy options for user access and passwords,
11. VCPProgrammer. VCPProgrammer is a PC based utility that allows the poll-worker to generate the Voter Access Card voters. The poll-worker selects the precinct and party and, if needed, identifies the ballot as a provisional ballot or set the Access Card to set up the Audio ballot. During Early Voting, this allows VCPProgrammer to create Voter Access Cards for voters in any precinct or party (in a Primary). If the program is used in a polling location that doesn't need all the precincts, VCPProgrammer cannot block out the unneeded precincts. During the volume test many of the errors detected could be attributed to the poll-worker selecting the wrong precinct or party. Procedures are needed for the poll-worker to confirm the card.
12. Slide contact. A test we use on touch screen devices is to slide the finger into the vote target area. In the earlier testing, we encountered system errors requiring the system to be reset or rebooted. None of the incidents resulted in a loss of integrity of the vote but the incidents were occurring frequently enough to cause concern. DESI discovered that, when the voter slide their finger in the final cast ballot action, the slide was not handled correctly and the DRE would complete the vote cast but not clear the system for the next voter. This problem and some similar problems were detected and corrected for this version.
13. ABasic Files. AccuBasic report files are used to configure AccuVote-OS and AccuVote-TS report contents and printing in precinct count mode. They are actually loaded into the memory cards for the AV-OS and AV-TS where their logic is executed. There are 24 report files supporting modifications to the reports for different states and jurisdictions. A few of these may provide options that are attractive to local jurisdictions as they provide variations on what summary reports are printed optionally or automatically and the order they are prepared. At the current time, the Federal testing only uses one of these files and does no source code review, leaving this to the states to verify. Within our state testing, we only verified the reports for the same file, 194US.abo, revision 1.15, and have checked the source files. Since the source file is not reviewed in the Federal testing, we have no absolute verification that the installed file found in the witnessed build (forwarded by Ciber) was created from these source files but signature information in the .abo file matches what would be expected from the source file.

The source code I was given clearly does not directly affect stored votes or even the voting result content of the reports. It just sets up the report options that will be available to the operator and some operator display information that sets up the options. The .abo file given is without risk to the election results.

The actual file used is selected in the AV-OS Options window of GEMS from the pull-down list in the Report field so the local user could potentially select any of these files or a modification of that file. The risk occurs in the opportunity to replace the verified file with some other .abo file (prior version, one the other existing versions installed in the GEMS/ABASIC directory, or by replacing the current code with rewritten code performing other operations.) In a certification report last year, we recommended that the unverified report files be deleted from the GEMS directory leaving only the verified

files. The California Use Procedures should specify which files are approved for use and provide information so that the approved files may be verified.

The risk involved with these files suggests that jurisdictions using this system should safeguard these files, as well as the election definition media that is used load these files to the voting machines.

HAVA Compliance

This system meets all the HAVA requirements that are defined and testable within the Federal Voting System Standards-2002. Beyond that, the Department of Justice has released an interpretation that basically states HAVA compliant systems are not expected to provide a completely identical and independent voting experience for every disabled voter; some may require assistance. The problem falls on the states to determine whether the support given by a particular voting system design provides sufficient support or whether more will be required. At this time, I do not have sufficient guidance to identify if the system is fully HAVA compliant pending a determination of what levels or types of support are sufficient. In some of the situations listed below, the decision may await court decisions based on existing lawsuits. Here are the borderline cases I have identified in this test:

- a. The AVPM, as an AVVPAT device, does not provide a blind voter with the opportunity to verify the vote using the paper audit record. Past precedence with other certified systems suggest that this should be accepted.
- b. The AV-TSx does not provide support for assistive devices for the physically disabled such as sip and puff or jelly buttons. There are different interfaces for these devices and no standard set yet which is universally accepted.
- c. DESI has suggested the use of mouth-sticks or similar device would allow physically disabled voters to use the touch screen. This option has not been tested and may also result in no AVVPAT record if it becomes necessary that the touch-screen is removed to place it within the operational reach of a mouth-stick.
- d. The magnifying lens for the AVPM view port resulted in some lines of the report being obscured. DESI removed the lens on the system last tested and suggested replacing them with a magnifying sheet lens. No criteria for visibility of the AVVPAT record has been established.

Conclusion

As configured and presented for testing, this version meets current standards for use in California with the following caveats:

- a. A decision to accept or deny on the HAVA compliance issues.
- b. Completion the California Use Procedures with following recommendations:
 1. Verification of AVPM firmware version needs to be included in acceptance testing.
 2. A copy of the audit report should also be printed and stored in the secure canister before the canister is removed from the TSX/AVPM at the conclusion of the election..
 3. The option to use the barcode in official elections should be turned off.
 4. The ABasic Report file should be restricted to 195US.abo, Version 1.15, and information provided to confirm the correct (unmodified) file is in use.
- c. Paragraph 6.3.y of Superior Court Case No. RG03 128466 needs to be completed and confirmed.

Sincerely,

A handwritten signature in cursive script that reads "Steven V. Freeman". The signature is written in black ink and is positioned above the printed name.

Steven V. Freeman

Attachments:

- A. List of the test configuration components
- B. Description of the Test Election.

Attachment A

Test Configuration Inventory

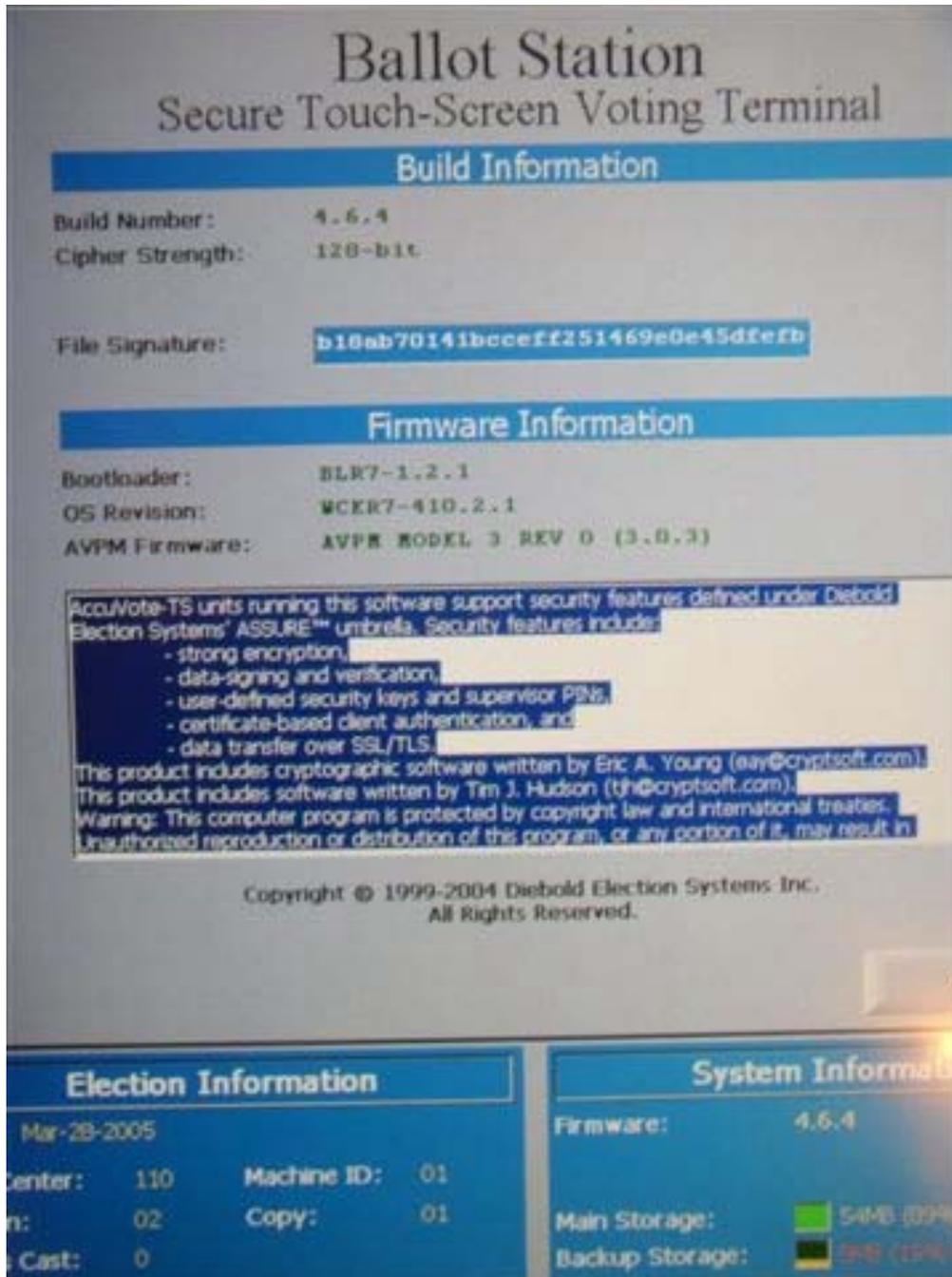
1. Dell Power Edge 600SC, HH18021 Chassis S/N
 - a. 1.8 gigahertz, Pentium 4 processor
 - b. 1 GByte RAM
 - c. 20 GByte IDE Internal Hard Drive
 - d. ViewSonic VE 155, 905035200089
 - e. PLEXTOR CD-R PX-W1210S SCSI CdRom Drive
 - f. 3.5 Diskette Drive
2. Hewitt Packard Laser 1020 Printer S/N: CNF B989445
3. Commercial-Off-The-Shelf Software
 - a. MS Windows 2000 Server, Service Pack 4 (Build 2195) w additional patches for SP5.
 - i. Window Internet Explorer 6.00.2800.1106
 - b. Adobe Acrobat Version 6.0.0.2003051900
 - c. Adobe Audition Version 1.0
 - d. Nero CD/DVD Rom Burning Suite, Version 6,
 - e. WinZip 8.1, SR1
 - f. McAfee SecurityCenter Version 5.0.0.0
 - g. McAfee VirusScan Version 9.0.0.0
 - h. SEIKO Epson Driver
 - i. (The application also includes Seagate Crystal Reports)
4. Diebold Election Systems, Inc. Software:
 - a. GEMS 1-18-24
 - b. Key Card Tool 4.6.1
 - c. VC Programmer 4.6.1
5. Voting Machines
 - a. AV-TSx Rev 7,
 - i. S/N 206132
 - ii. S/N 204806
 - iii. S/N 204905
 - iv. S/N 226724
 - v. S/N 203637 (also tested with BS 4.6.3)
 - vi. S/N 203203 (used to test copying results from one DRE to another).
 - vii. S/N 212998 (used in copying results as an accumulator)
 - viii. S/N 225636
 - ix. S/N 213242
 - x. S/N (not recorded)

These machines were used for specific tests and final consolidation report.
Half had precincts 1 and 2 (both splits) and the half had precincts 3, 4, and 5.
 - b. Ballot Station Firmware Ver. 4.6.4,
 - c. AVPM Model 3 Rev 0 (3.0.3) (See note 1)
6. Documentation
 - a. GEMS 1.18 Users Guide, Revision 12.0
 - b. GEMS 1.18 Reference Guide, Revision 8.0
 - c. GEMS 1.18 Election Administrators Guide, Revision 8.0 [9]
 - d. GEMS 1.18 Server Administration Guide, Revision 3.0.
 - e. GEMS 1.18 System Administrators Guide, Revision 6.0
 - f. AccuVote-TSX Hardware Guide, Revision 8.0
 - g. AccuVote-TSX Pollworkers Guide, Revision 4.0 [5]

- h. Key Card Tool 1.0 Users Guide, Revision 2.0 [Key Card Tool 4.6 Users Guide Rev 1.0]
 - i. Voter Card Encoder 1.3, Users Guide 2.0 [1.0?]
 - j. VCProgrammer 4.1 Users Guide, Revision 4.0 [VCProgrammer 4.6 Users Guide Revision 1.0]
 - k. AccuVote-OS Hardware Guide, Revision 6.0
 - l. AccuVote-OS Pollworkers Guide, Revision 3.0
 - m. AccuVote-OS 1.96 Precinct Count Users Guide, Revision 3.0
 - n. AccuFeed 1.0 Hardware Guide, Revision 1.0
- [Note: the references in brackets [] are updates that have been listed by DESI but were not provided as part of this test.]

Configuration Notes:

1. The model identification provided for the AVPM comes from the Diebold Assure Umbrella report, an online report of installed versions and security settings available to the election official in the BS Ver. 4.6.4.



On the AVPM unit itself, the model number may be found on the strip under the paper source roll. There is no model number labeled externally where is easily verified.

2. The ABasic 195US.abo file version can be found by opening the file with a text editor and checking the first line. The field highlighted below shows the version.

F "abAgPa **US 1.15** ObbOcpBhLahOdaPb'OS'Pc'CARD 'E.=NeWeSaaabb'4"

This will not necessarily catch a modified file. A stronger test is to use a hash program to generate one of the following hash values:

CRC-32 793A7172

MD5 47825805CC00A5717AF8CAF1F128A646
SHA-1 3A987D976D784A2C70D7908CA85A85C822B47BC5.

Attachment B.

Test Election Design

Precinct	1	2	3	4	5
Split		1	2		
Presidential	x	x	x	x	x
Federal, STATE, or COURT	x	x	x	x	x
Board of Equal 3	x	x	x	x	x
CONGRESS 49	x	x	x		
CONGRESS 50				x	x
CONGRESS 51					x
STATE SENATE 35	x				x
STATE SENATE 37		x			
STATE SENATE 39				x	
ASSEMBLY 66	x				
ASSEMBLY 74		x	x		
ASSEMBLY 75				x	
ASSEMBLY 76					x
ASSEMBLY 77					x
COUNTY, Unincorporated		x			
CHULA VISTA			x		
LEMON GROVE	x				
PORTER VISTA				x	

Political Parties	Abbrev.	Major	Minor	DTS
American Independent	AI		x	X
Democrat	DEM	x		X
Green	GRN		x	
Libertarian	LIB		x	
Natural Law	NL		x	
Peace & Freedom	PF		x	
Republican	REP	x		X, except Presidential race

The primary election included a total of 102 different candidates or choices distributed among 55 contests, including Presidential nomination, vote for 2, judicial recall, and measures. The general election included 31 contests with 82 candidates/choices.

Languages:

English, Spanish, Chinese (Vietnamese was used in the May and June testing)
 (Spanish, Chinese, Korean, Japanese, Vietnamese, Tagalog, and Creole were tested in ITA testing)

The same primary and general test elections were used in all four test events. A special election based on the Governor Recall race was also used in the earlier test to confirm that the AV-TSX can correctly handle multiple page ballots. In the final volume test and all previous test events, uploads were made to test consolidation and final reporting using GEMS. The uploads during the volume tests used only a subset of the DREs and specifically included the units which were used to run specific test procedures listed below.

A total of 1100 ballots were cast among the ten test units for the Primary election. The General Election was used to test Audio and language ballots and some special tests to confirm behavior in various voter error conditions or loss of power.

2. Regression and change test.

After the volume test, three DREs were pulled and additional test ballots run to check problems, changes, or features that were not used or observed in the volume test. One of the DREs (S/N 203637) was set up with a prior version of the ballot station software to show and verify actions that resulted in problems in that version, a second DRE (S/N 203203) was used which duplicated the voter actions on the first but using the ballot station version which was being tested for certification. The third DRE (S/N 212998) was used to perform actions involving checking memory cards, resolving provisional ballots, recovering ballot images, consolidating results from multiple DREs in a single polling place or vote center into a single combined total for upload, and using a master DRE to upload results from other DREs.

Among the specific tests conducted were:

- a. Automated L&A test.
- b. Provisional ballots in different precincts and parties.
 - (1) Provisional ballots in both splits of the split precinct.
 - (2) Write-ins in provisional ballots.
 - (3) Identifying provisional ballots when reviewing ballot images
 - (4) Provisional ballots for both partisan ballots by partisan voters and by DTS voters.
 - (5) Accepting provisional ballots in an accumulating DRE (as opposed to accepting provisional ballots in GEMS). This involved returning the memory card to the original DRE and confirming the accepted provisional ballot remains accepted for recovery.
- c. Sliding finger/multiple touches on various 'buttons' and areas of the voting screens. (This test has been done before but was important in this case as it was discovered after the July volume test that a tester sliding the finger into the button area was causing a number of system errors requiring the DRE to be rebooted.)
- d. Write-in problems observed in earlier releases:
 - (1) Changes in the keyboard (removing Tab and ...)
 - (2) Multiple blank spaces in between first and last names
 - (3) Use of unusual characters such as (), [], and { } pairs, quotes, dashes, slant '/', question mark. (A fuller test was done in an earlier session involving all the special characters but this test specifically tested characters that were known to cause problems in the past).
 - (4) Sliding finger on record and cancel buttons.
- e. Basic navigation to go forward, back, access summary screen directly, change previously voted candidates to alternate candidates (the voter correcting a misplaced vote), undervoting races.
- f. Rejecting a printed ballot twice and then automatically casting the ballot on the third attempt.
- g. Checking operational options that occur when a paper tape roll gets too low or runs out.
- h. Pulling the voter access card before completing voting.
- i. Using the VCP elements located under supervisor control on the DRE (third DRE) to create access cards.

j. DCR print diagnostics and take-up paper options.

Previous tests also included:

- a. These same tests in English, Spanish, Chinese, and audio ballots.
- b. The use of long write-in names trying to overrun the buffer (the buffer is truncated at about 255 characters).
- c. Disconnecting power cables in the middle of voting.
- d. Pulling and replacing the memory card.
- e. Timeouts.
- f. Attempting to pull the voter access card before casting ballot.
- g. Verifying operation of the Key Card Tool, Vote Card Programmer, and VCE. This included verifying the strength of the password/pin numbers and checking the encryption keys.
- h. The volume test included checking the ability to correctly count every ballot voting choice including multiple write-ins and some unvoted options. All access cards were created using VCP.

Test on consolidating results on a single DRE.

Used Machines S/N 203203 (voted) 212998 (accumulator).

1. In printing the summary report from 203203 on 203203, two incidents occurred where the font changed size and squeezed lines together. One line is overwritten to the point that it is nearly unreadable.
2. Audit log printed on accumulator (212998) with the 203203 memory card installed includes 203203 audit log embedded. The obverse is also true; moving the memory card back to 203203 and printing audit log picks up the audit log from 212998.
3. Audit log reported printer failures due to low paper sensed.
4. Audit log shows use of Administrator card and pin, including attempted use of improper pin.
6. Ballot images print with barcode.
7. Backup recovery reported in the audit log along with electronic hash signature