Voting System Examination
Dominion Voting Systems Assure 1.3

Prepared for the
Secretary of State of Texas

James Sneeringer, Ph.D.
Designee of the Attorney General

This report conveys the findings of the Attorney General's designee from an examination of the voting equipment listed below.

Examination Date	August 22-23, 2012
Report Date	September 18, 2012

Components Examined

		EAC/NASED Qualification	
Component	**Version**	**Date**	**Number**
Global Election Management System (GEMS), Central Count	1.21.6	June 29, 2012	DVS-Assure1.3
AccuVote-OS (Precinct Count) with new Memory Card	1.96.14	June 29, 2012	DVS-Assure1.3
AccuVote-OS (Central Count)	2.0.15	June 29, 2012	DVS-Assure1.3
AccuVote-TSX & TS Ballot Stations	4.7.10	June 29, 2012	DVS-Assure1.3
TSX WinCE	4.10.3.10	June 29, 2012	DVS-Assure1.3
TS WinCE	300.3.5	June 29, 2012	DVS-Assure1.3
TSX/TS Bootloader	1.3.11	June 29, 2012	DVS-Assure1.3
Key Card Tool	4.7.8	June 29, 2012	DVS-Assure1.3
ABasic	2.2.5	June 29, 2012	DVS-Assure1.3
Voter Card Encoder	1.3.3	June 29, 2012	DVS-Assure1.3
VC Programmer	4.7.8	June 29, 2012	DVS-Assure1.3
Cardwriter	1.1.6	June 29, 2012	DVS-Assure1.3
PCS Central Count Scanner	2.2.5	June 29, 2012	DVS-Assure1.3
Assure Security Manager	1.2.5	June 29, 2012	DVS-Assure1.3

Voting

Election Setup	PCMCIA or 40-pin memory card. Nothing is pre-programmed in the terminals; all the election information is in the memory card.
Zero-total report	Yes, on the thermal printer.

Authorization to vote / Ballot selection	Voter cards (smart cards), which authorize voting, are generated by · A handheld Voter Card Encoder (up to 8 ballot styles), · A laptop running VC Programmer software, or · An AccuVote R6 (occasionally). A manager card and password are used to authorize a machine to generate voter cards. The voter cards are automatically cleared after voting, so they cannot be reused.
View / Vote	LCD display / touch screen
Vote Storage	Internal flash memory and on the PCMCIA card.
Transfer Results	PCMCIA or 40-pin memory cards, depending on the device.
Print precinct results	Yes, on paper tape printed at the voting station.
Straight party / crossover	Yes. Cancelling a straight-party vote does not affect any crossover votes.
Provisional Ballots	The poll worker can designate a ballot as provisional and enter a number that will identify the ballot so it can later be included in or excluded from the count. The voting station will verify that the ballot ID is a valid one, preventing most entry errors, but duplicates are not detected unless the same voting station is used.
ADA	Yes, but see Concern number 8 below.
Curbside Voting	Yes. The voting tablet can be removed from the stand and carried to the curbside.
Note	Each voting station is an independent stand-alone system, which cannot communicate with other stations or election central except when the polls are closed.

Election Setup / Tabulation

Results Storage	Encrypted, proprietary database on the hard drive.
Tamper Resistance	The data is encrypted and the OS is locked down during tabulation, but see Concern number 5, below.
Real-Time Audit Log	Yes, but it does not meet the requirements in the Texas rules. See Concern number 6 below.

Changes

- They now have the Assure Security Manager (ASM), software that runs on a separate machine and determines the rolls that are permitted for each user ID.
- An authentication code is required to install their software on a different computer, presumably to prevent piracy of their software.

Comments

- Dominion recommends that only the necessary Dominion components and computers be allowed on the local area network (LAN) with the GEMS computer, for security reasons. I wholeheartedly agree, and suggest that this procedure always be followed.
- Dominion has a ballot marking device, called Automark, which was not presented for certification and should not be used in Texas.
- Dominion has a voter-verified paper audit trail feature, but they did not present it for certification in Texas, and therefore it should not be used in Texas.

Concerns

1. **Scanner Accuracy.** Dominion declined to reveal the test plan used by SLI Global Solutions to test scanner accuracy. Therefore, the examiners cannot judge scanner accuracy without repeating the extensive testing done by SLI. Dominion should provide this information.
2. **Scanner Jams.** The PCS Central Count Scanner frequently stopped due to paper jams, even with the small number of ballots we ran. Dominion told us that the scanner they brought had been around their office for a while and was not in good repair. However, if a vendor cannot bring a working scanner to an examination, how can we have confidence that they can deliver working equipment to customers?
3. **Incorrect labels.** We tried to verify that the precinct scanners that Dominion brought to the examination were actually the versions that we were supposed to be examining, using Dominion's documentation to identify them. We found that one of them did not have the proper labels. Dominion assured us that it was the correct version, and explained that it was an old machine that was around the office, and they upgraded to the correct version before bringing it to the examination, but forgot to label it properly. In my opinion, an ISO 9000 certified manufacturer of election equipment should be able to bring properly labeled equipment to an examination. Being able to correctly identify the version of a piece of equipment is an essential part of running secure elections.
4. **Access to Audit Logs.** The Dominion system maintains electronic audit logs, but they are quite difficult to actually audit. Each voting station keeps such an electronic log and stores it on the memory card at the end of the election, as well as retaining it within the voting station. It is stored in encrypted form, which protects it from tampering, but also makes it difficult to read. The audit log can only be viewed by printing it on paper tape, either on the voting station that generated it, or on another station that has been configured for the same election. These are slow printers, so this can take a very long time, especially if you include the time to start the machine and the printout. Also, since the logs are paper, a person must scan them visually to locate anomalous events. This is a tedious, error-prone process, and it is therefore all but impossible to detect any anomalous events on the night of the election.

   It should be possible to automatically flag anything unusual, or to perform automated searches or queries on the log file. For example, it should be possible to automatically locate early or late poll openings or excessive scan error rates.

   Dominion took the position that the law only requires that there be a log, and does not say how it should be provided or that it be conveniently available.

5. **Access to the Operating System.** Texas rules require that there be no access to the operating system (in this case Windows) during tabulation. Although GEMS enforces this, it is implemented using features of Microsoft Windows, and can be turned off by anyone with Windows administrative rights, provided GEMS has not been started. (Once GEMS has been started, it is no longer possible to defeat this.)

   According to Dominion they have taken these actions to address the problem: (a) shipping systems that are properly configured, (b) publishing procedures for properly configuring Windows, and (c) restricting Windows administrative rights.

   This is not sufficient in my opinion.

   Item (a), above, is not that helpful, because not every customer purchases the hardware from Dominion.

   Item (b) is not practical, because the required steps fill a nine-page, single-spaced document entitled "Protecting Windows 2003 Server for Texas's (sic) GEMS server," which present quite a challenge to typical jurisdictions. The steps are not simple ones. For example, on page 2 in the section labeled "Explorer," the second step is "Allow Running Only Certain Applications." The allowed applications are not specified, and no further details are given. I am a longtime Windows user who holds a Ph.D. in computer science, and I would need reference materials or other help to figure out how to do that.

   On the other hand, the instructions on pages 5 - 7 can be accomplished relatively quickly by following the six detailed steps on page 5.

   Item (c) does help somewhat by restricting the people who can tamper with the system to those who have administrative rights, but it still does not meet the requirement.

   Restricting operating-system access is not a critical security feature, but it is required in Texas, and the procedure is so onerous that I doubt it is often carried out. GEMS should ensure compliance by refusing to tally real votes unless operating system access is actually disabled. (For example, when GEMS starts, it could check that the proper Windows settings are actually in force, so that OS access is known to be actually disabled. If they are not in force, GEMS could refuse to run.)

6. **Real-time Paper Audit Log.** Texas has a requirement for a real-time audit log on a continuous-feed printer. GEMS has a paper audit log, but it is does not meet the Texas requirements. Texas requires that the tabulation system stop working whenever any log entry cannot be printed as soon as the event occurs. (This is the meaning of *real time*.) Also, any interruption in the real-time logging must itself be logged.

   Here are the technical details: During the exam, we took the printer offline and demonstrated that GEMS continued to function. Only when we put the printer back online, did it print the log entries. The taking of the printer offline was not logged. In another test, we took the printer offline while a number of events occurred. Then we switched the power to the printer off and then back on. While the printer was powered off, GEMS refused to process anything and a prominent message was displayed explaining the problem. However, GEMS permanently lost the log entries for all the events that occurred while the printer was offline, and the fact that the printer was offline and then powered off was itself not logged.

   This is not a critical security feature, in my opinion, but it is explicitly required in Texas, and the Dominion GEMS system does not comply.

7. **Expiration dates ignored on security certificates.** There is a small risk in the Assure 1.3 system, because it ignores the expiration dates on its security certificates, allowing

certificates to continue to be used after they are expired. Security certificates (like passwords) have expiration dates in part so the damage can be contained if a certificate is compromised, and Assure lacks this protection.

To understand this requires understanding the history of the Assure system. Contrary to best practices, the root certificate is integrated into the software, so a new software version (and therefore new regulatory certification) is required to use a new certificate. To prevent this problem in the future, Dominion has changed the software to ignore the dates on the security certificates, and accepted the risk that this entails.

Since the older systems do not have this workaround, they will stop functioning when their certificates expire. This means that all Dominion (or Diebold or Premier) voting systems in Texas will stop working in July, 2013, or January, 2014.

8. **ADA Compliance.** The examiner who tested the audio reported excessive static on the Accuvote-TS, making it very difficult to understand. Also, the voter must press the key to cast the ballot before he can use the audio to review his ballot. Texas law requires that a voter be able to review his ballot before casting it.