



FREEMAN, CRAFT, MCGREGOR GROUP



Report from a Review of the
Voting System in
The State of Maryland

Prepared October 12, 2006

Introduction

Chapter 564 of the Laws of Maryland (2001) requires the selection and certification of a uniform statewide voting system for polling place voting and a uniform statewide voting system for absentee voting. By 2006, all jurisdictions in Maryland are required to use the uniform voting system. The State Board of Elections (SBE) chose the Diebold Election Systems, Inc. (DESI) AccuVote-Touch Screen (TS) for polling place voting and the Diebold AccuVote Optical Scan for absentee voting. Implementation of the system has been in three phases beginning with installation in four counties for use in the 2002 election and nineteen counties for the 2004 election. The final jurisdiction, Baltimore City, has installed the system for the 2006 elections.

In a report dated July 23, 2003, entitled “Analysis of an Electronic Voting System,” (the Rubin report) computer scientists from Johns Hopkins University and Rice University stated results of their analysis of source code for a DESI voting system. The report addressed security issues and vulnerabilities of DESI source code that was found on a DESI web site.

Much has been written by others both pro and con regarding the value and accuracy of the Rubin report. The significance for the State of Maryland is that the Rubin report triggered a process of ongoing evaluations of the voting system and the procedures the state of Maryland uses with the system. The State Board of Elections has been very proactive, attempting to fairly and responsibly address every criticism, finding and recommendation regarding their system. This continued process of critique and evaluation, followed by changes to address the issues raised, may have now given Maryland one of the most secure and reliable voting systems in the nation.

Following the publication of the Rubin Report, Maryland Governor Robert L. Ehrlich, Jr., directed that an independent review of the security of the Diebold AccuVote-TS Voting System and the election processes surrounding it be performed. The Department of Budget and Management (DBM) and the SBE jointly managed the project. Science Applications International Corporation (SAIC), performed the analysis and issued its report on September 2, 2003.

On November 10, 2003 the Department of Legislative Services, Maryland General Assembly of the State of Maryland (DLS) entered into an agreement with RABA Technologies, LLC to perform a “trusted agent” evaluation of certain aspects of the State Board of Elections plan to use touch-pad “Direct Recording Electronic” (DRE) devices for upcoming elections. RABA issued its report on January 20, 2004.

In 2005, Governor Ehrlich established the Governor's Commission on the Administration of Elections a group tasked to study legislative proposals for election administration. The Commission issued an Interim Report on January 9, 2006

In July 2005, the State Administrator of Elections contracted for a study of independent verification systems. The study included a review and evaluation of independent verification systems, including at least one voter verified paper audit trail, for the State's current touchscreen voting system. The SBE also contracted with the Maryland Institute for Policy Analysis & Research at the University of Maryland, Baltimore County to conduct a study on Voters' Opinions About Voting and Voting Technologies, Vote Verification Technologies and Usability of Vote Verification Systems. Their reports were issued in February 2006

In December 2005, new security risks within the ABasic code used by the Diebold system were discovered. The mitigations for the risks of this weakness in the system have been well documented. Several states including Maryland have evaluated and began implementing procedures to address those risks.

On April 27, 2006, the SBE entered into a contract with the Freeman Craft McGregor Group to perform a review as described in the Objectives section below. This is the report of our review.

Objectives

As titled, this is a report of a review of the voting system implemented in the State of Maryland. The objective of this review is to assist the Maryland State Board of Elections by providing an independent review of specific areas that the Board and other stakeholders have identified and requested that we review. The use of this report for any other purpose may lead the user to ill-founded conclusions.

The specific objectives are:

- Review the Diebold Election Systems voting system configuration used in Maryland that consists of the following components: Global Election Management System (GEMS), AccuVote TS R6, AccuVote Optical Scan, Voter Card Encoder, and Key Card Tool.
- Address the AccuBasic issues by comparing the version of the system used in Maryland to the version examined and recently certified by the State of California and determine to what extent the findings and recommendations in the California reports are applicable to the configuration of the systems which are used in Maryland.
- Compare the installation and operation of the firmware on the TS R6 used by Maryland with the TSX with Verifiable Voter Paper Audit Trail (VVPAT), as used in California, to determine if there are different security risks between the two hardware designs.

- Review the findings of report issued by the Science Applications International Corporation (SAIC) to see if any of the vulnerabilities identified have not been addressed by Diebold or within the State Board of Elections' Information System Security Plan (ISSP).
- Review the findings of the report issued by RABA to see if any of the vulnerabilities identified have not been addressed by Diebold or within the State Board of Elections' Information System Security Plan (ISSP).
- Review the ISSP and Maryland's election procedure documents for security vulnerabilities or other risks to the accuracy and reliability of the system which have not been addressed.
- For any unaddressed risks that are found, provide recommendations for specific actions to mitigate those risks.

The intended users of this report are election administrators and those stakeholders responsible for enacting election law, formulating policy, funding and budgeting for the election administration programs.

We are well aware that our clients may choose to publish this report. With that understanding, we have attempted to use terms and descriptions that will be understandable to readers who are unfamiliar with election administration and to minimize the inclusion of any confidential information which would require redaction prior to publication.

Findings and Recommendations

Review the Diebold Election Systems voting system configuration used in Maryland

The configuration of the Diebold Election Systems' equipment used in the State of Maryland includes the following components:

- Global Election Management System, Version 1.18.24
- AccuVote Optical Scan units with firmware version 1.96.6
- AccuVote TS6 Touch Screen voting unit with firmware version 4.6.4
- Key Card Tool 4.6.1
- Voter Card Encoder, firmware version 1.3.2

The system is configured for polling place voting on the TS6 touch screen units and the tabulation of absentee and provisional ballots in the Local Boards of Elections (LBE) on the optical scan units. Election definitions are created on the State's installation of GEMS and are distributed to the counties. The election office in each county reviews and proofs the election definition provided by the State. When the county decides that the definition is acceptable, they load it onto their local installation of GEMS to program their equipment. The Key Card Tool, which provides the encryption keys, resides solely

with the State. The State prepares the key cards with new keys for every election and distributes them to the counties.

We conducted system validation procedures on the State server and on the servers in Harford, Howard, and Kent Counties. We found that all four servers had the required elements for GEMS version 1.18.24. We found some files remaining from prior versions of the system as well as variations in touch screen text display files and audio files. We understand that the text files and audio files were modified by the State to improve usability and accessibility.

We conducted system validation procedures on all of the optical scan units and a sample of the touch screen units in Harford, Howard and Kent Counties. The optical scan firmware was off loaded, compared and found to be identical to the trusted build of the firmware provided by Wyle Laboratories. In each county, a sample of the touch screens was booted up and the file signature was verified to be identical to the signature of the trusted build of the version 4.6.4 firmware.

Details of these findings and recommendations were reported to the Maryland Board of Elections on June 30, 2006.

Applicability of the findings and recommendations in the California AccuBasic reports to the configuration of the system used in Maryland

The firmware versions in the Maryland configuration of the system are the same as the versions included in the system certified by the California Secretary of State on February 17, 2006. Although the Maryland system uses a TS6 touch screen and the California certified system uses the TSX touch screen with the AccuView Printer Module, the firmware versions are the same. Accordingly, the findings and recommendations relating to the AccuBasic firmware addressed in the California reports are applicable to the system configuration used in Maryland. At the time of our examination, Maryland's procedures for the security of the memory cards and the mitigation of risks identified in the California report were being drafted. We reviewed a draft of those procedures and provided written recommendations to the Maryland State Board of Elections on July 17, 2006. The procedures were published on October 2, 2006. In our review of the published document we found that the recommendations we made in our July 17, 2006 review of the earlier draft had been implemented.

Comparison of the TS R6 used by Maryland with the TSX with VVPAT as used in California

A side by side functional and physical comparison of the AccuVote TS6 and the AccuVote TSX was conducted.

The most significant difference is that the case of a TS6 unit, when properly assembled, cannot be opened unless the memory card door is unlocked. One of the screws holding

the case in place can only be accessed when the memory card door is open. In addition, when the memory card door is locked, the memory card cannot be removed or replaced without aggressively disassembling the unit. While this makes an attack on a TS6 by opening the case to bypass the lock on the memory card door much more difficult than on the TSX, we recommend that Maryland continue its use of tamper evident seals on the case of the TS6.

The case of a TSX unit can be opened while the memory card door is locked. Once the case is opened, the memory card can be removed and replaced and the case reassembled without unlocking the memory card door.

The TS6 takes a PCMCIA modem card. The TSX modem is internal. The two machines have different communications bays.

The TSX has a memory card locking door and a communications locking door. The modem port and the network port are both located behind the communications door. The memory card bay and the on/off switch are both located behind the memory card door. The TS6 has one door that covers the memory card slot, the combined slot for the modem and network card, the on/off switch, a PS2 keyboard port and a (disabled) IR port. Both machines require opening the memory card bay to reach the on/off switch and power up the machine. On the TSX touching the "Shut Down" button on the screen will power down the machine. On the TS6 touching the "Shut Down" button on the screen returns a message that the machine is ready to be powered down.

The keyboard connection on the TS6 is usable but is restricted to the input being allowed on each screen. It exists only as an alternative to touching the screen for employees who are performing maintenance operations on the equipment. We were able to use the combination of the Control – Alt – Delete keys to end the process and shut down the machine. In certain menus, it is possible to navigate from one button to another with the key and activate a selected button with the return key. In the save macro file, where there is a keyboard entry painted on the touch screen, the keyboard is allowed to use those keys shown on the screen. We found no functions available through the keyboard beyond those available through the touch screen interface and the on/off switch.

We could not compare installation of the Ballot Station firmware because we did not have an install file for the TSX firmware.

Other differences in the two machines include:

There are very obvious physical design differences, including the AccuView Printer Module on the TSX, which provides a voter verifiable paper audit trail and which is not available on the TS6.

The TSX has a more vertical design, with the voter card port on the upper right of the machine. The TS6 has a horizontal design with a screen that tilts up toward the voter and the voter card port on the lower right side of the machine.

The TS6 has an option for using a landscape configuration on the screen. The TSX does not allow the landscape configuration

The calibration screen on the TSX has a copyright on it. The TS6 does not.

The two models use different processors. The TS6 has a Hatachi SH3 processor, while the TSX uses an ARM 720 processor.

The operating system in the TS6 is 3.0, Build 126. The operating system in the TSX is 4.10 Build 908

Memory and storage in the TS6 are 18MB and 9MB. The TSX has 33MB and 44MB

The file signature value for the TS6 with version 4.6.4 firmware is:
4a3fcb503eb328e1c6beef66a94f2d69.

The file signature value for the TSX with version 4.6.4 firmware is:
b18ab70141bcceff251469e0e45dfefb.

The options for audio diagnostics are different between the two models. The TSX offers a selection between speaker and headphone. The TS6 only offers the speaker option. The TS6 automatically disables the speaker and plays to headphones when the headphones are installed. The TSX allows the use of either one.

Review of the implementation of the recommendations in the SAIC report

The SAIC report recommended that the State Board of Elections implement certain mitigation strategies to bring the AccuVote-TS voting system into compliance with the State of Maryland Information Security Policy and Standards. Their recommendations are shown as bulleted items below. Our comments are within the indented paragraphs following each bulleted item.

The SAIC mitigation strategies were:

- Consider creating a position for a Chief Information Systems Security Officer (CISSO) position at the State Board of Elections. This individual would be responsible for overseeing the security of operating the AccuVote-TS voting system.

This was addressed with the creation of a Chief Information System Security Officer and filling that position.

- Develop a formal, documented, complete, and integrated set of standard policies and procedures. Apply these standard policies and procedures consistently through the Local Board of Elections in all jurisdictions.

This has been implemented.

The State Board of Elections' "Conducting the Election Guide" provides Local Boards of Elections with standard procedures for ballot production, logic and accuracy testing, Election Day process and canvass. This document was published after the SAIC report. Document history logs reflect updates this past spring in preparation for the 2006 elections.

The board has developed and implemented new procedures to deal with the Diebold memory card issue and the firmware upload issues recently discovered.

- Create a formal System Security Plan. The plan should be consistent with the State of Maryland Information Security Policy and Standards, Code of Maryland Regulations (COMAR), Federal Election Commission (FEC) standards, and industry best practices.

This recommendation was implemented on June 30, 2004. The July 7, 2004 version of the plan reflects progress on items as described below. An update of the plan was initiated on March 14, 2006 and is in a final draft form and is being reviewed for adoption.

- Apply cryptographic protocols to protect the transmission of vote tallies.

This process has been completed.

- Require 100 percent verification of all results transmitted to the media through a separate count of PCMCIA cards containing the original votes cast.

This process has been completed.

- Establish a formal process requiring the review of audit trails at both the application and operating system levels.

This process has been completed.

- Provide formal information regarding security awareness, training, and education programs appropriate to each user's level of access.

This process has been completed.

- Review any system modifications through a formal, documented, risk assessment process to ensure that changes do not negate existing security controls. Perform a formal

risk assessment following any major system modification or, at a minimum, every three years.

Since the September 2, 2003 Risk Assessment by SAIC, the system modifications have been executed through the implementation of recommendations and have been made with the intent to enhance existing security controls. Although there have been no system modifications that meet the definition of “major system modifications”, the three year cycle recommended would have been completed on September 2, 2006.

The SAIC report was conducted in an odd numbered year, between elections. Attempting to conduct a risk analysis of the same scale and scope during an even numbered election year would take precious resources within the State Board of Elections away from the tasks of election administration and introduce greater risks into the process.

However, a limited scope review such as we have performed cannot begin to provide the same level of thorough examination and assurance as the SAIC report. Accordingly, we do not believe that our review meets the intent of the SAIC recommendation. We recommend that the State Board of Elections perform a formal risk assessment as soon as possible following the 2006 General Election. Conducting and completing such an assessment early in the spring of 2007 would allow fresh assessment of the policies, procedures and training used in the 2006 election. Publishing an analysis of that performance late in the spring would give the Board of Elections a year to implement recommendations before the next major election cycle begins. A full scale assessment in the spring of the odd numbered years before presidential elections and a limited scope review in the odd numbered years before non presidential elections might prove to be a workable solution.

- Implement a formal, documented process to detect and respond to unauthorized transaction attempts by authorized and/or unauthorized users.

This process has been completed.

- Establish a formal, documented set of procedures describing how the general support system identifies access to the system.

This process has been completed.

- Change all default passwords and passwords printed in documentation immediately. Verify through established procedures that the ITA-certified versions of software and firmware are loaded prior to product implementation.

This process has been completed.

- Remove the State Board of Elections GEMS server immediately from any network connections. The server should be rebuilt from trusted media to ensure and validate that the system has not been compromised. All extraneous software that is not required to operate the AccuVote-TS should be removed. The server also needs to be moved to a secure location.

This process has been completed.

- Modify procedures for the Logic and Accuracy (L&A) testing to include testing time-oriented exploits (e.g., Trojans). [Redacted]

This process has been completed.

- Discontinue the use of an FTP server to distribute the approved ballots.

This process has been completed.

- Implement an iterative process to ensure that the integrity of the AccuVote-TS voting system is maintained throughout the lifecycle process.

This process has been completed.

Review of the implementation of the recommendations in the RABA report

We were particularly concerned about the Red Team Exercise performed by RABA. Red Teaming has traditionally referred to the role of the adversary or simulated enemy in military war game exercises. It is now used by many government agencies and businesses for tasks including peer reviews, playing devil's advocate, and introducing alternative policies and interpretations into organizations. In information system security the term Red Team has commonly been interpreted as described in "Gray Hat Hacking, the Ethical Hacker's Handbook" (McGraw Hill/Osborne ISBN 0-07-225709-1 © 2005), which describes red teaming as

"...simulating a covert adversary skilled in the art of exploiting systems and social engineering.

There are different philosophies on red teaming but to properly simulate the adversary, a red team should not be given a network drop and an office across the hall from the IT team. A good red team should find its own access onto the network and, if possible, remain hidden throughout the engagement."

Based upon this understanding of Red Teaming, it would sound as if the RABA team was able to easily hack into Maryland's Diebold systems and exploit them. This was our

impression based upon popular press accounts prior to reviewing the RABA report. What the RABA report describes is very different. The report says:

...it was determined that a Red Team exercise be held to completely test and stress the exact system to be deployed for the March primaries. This exercise was held on 19 January 2004. For approximately one week prior, RABA's Innovative Solution Cel (RiSC) augmented with consultants from the University of Maryland and U.C. Davis were given copies of the source code and access to both a GEMS server and six AccuVote-TS terminals.

And;

The team focused on smart card vulnerabilities, AccuVote-TS terminal security, GEMS server security, and the methods used to upload results following an election. Since the scope of the effort was contractually limited (in dollars) the team's focus was necessarily directed toward the most likely vulnerabilities. Indeed, the total software package contains roughly 285,000 lines of source code, only a fraction of which could be carefully studied. In all cases the team first approached the system with no foreknowledge of the source code. As the attacks became more sophisticated, an increasing in-depth understanding of the actual system was necessary.

While the RABA Red Team Exercise appears to have provided an in depth analysis of security vulnerabilities in the four targeted areas of the system's security, the exercise does not appear to have been designed to simulate and estimate the risks of penetration of the "outsider adversary." The emphasis appeared to be determining what risks existed and what level of penetration and access would be needed to for an adversary to exploit them.

The RABA report provided the State Board of Elections a number of recommendations to improve the system. Their recommendations are shown as bulleted items below. Our comments are within the indented paragraphs following each bulleted item.

The RABA recommendations were:

- Create Security Key Cards with unique passwords by "precinct." and update all the Encoders and AccuVote – TS terminals within each precinct.

This was not implemented by "Precinct." SBE creates Key Cards for each election with unique passwords by "County." The SBE decided that the logistical risks that would be introduced by issuing unique keys for each precinct were too high.

- Apply Tamper Proof Tape to AccuVote-TS terminals to prevent non-authorized entry of Security Key Cards into the terminals. (The recommendation references the next section of the report)

Because key cards are a smart card, similar to the voter activation card and are read in the same card reader as the voter activation cards, the step required by this recommendation is not really possible and would make it impossible to insert voter activation cards and vote. The referenced next section of the report discusses the sealing of all locking bays of the machine, not the smart card reader slot. Accordingly we assume RABA intended this to prevent unauthorized entry of memory cards into the terminals.

In theory, unauthorized re-keying of a terminal to a key which differs from the key for the election could create a denial of service attack on the specific machine which was re-keyed. However, as RABA describes, machines cannot be re-keyed while in election mode with a memory card installed. Insertion of a key card during election mode is simply rejected because the machine is looking for voter access cards. If the machine were re-keyed prior to installing the memory card for an election, it would be unable to read the card and would need re-keying before it could be used.

Assuming this recommendation was actually referring to memory cards, then this recommendation has been implemented.

- Institute strict procedures to prevent the use of unauthorized Supervisor Cards.

This recommendation has been implemented by setting physical and procedural controls over the custody and use of Supervisor's cards.

- Secure physical access to the voting terminal using serial numbered tamper tape, and setting up procedures for periodic and routine inspection of the tapes.

This recommendation has been implemented.

- Place alarms on the locked doors of the PCMCIA card bay.

This has not been implemented. This would be a design change to the system which Diebold would need to implement and have certified.

- Remove the recording software from the AccuVote –TS Terminal.

This recommendation has been implemented.

- Investigate the legal implications of tampering with the hardware systems (such as jamming the card reader and disconnecting the monitor). Clearly post rules that indicate the consequences of such actions.

This recommendation has been implemented.

- Install all known security patches from Microsoft on the GEMS servers.

This recommendation has been implemented but is an ongoing process as security patches are rolled out over time. At the time of our fieldwork the SBE had not yet begun its final tour of the counties to install patches prior to the September primary. Installation of GEMS server security patches are a routine part of the process of preparing the LBE GEMS Servers for each election.

- Ensure modem access to GEMS is enabled only when uploads are expected.

This recommendation has been implemented. However, the RABA recommendation includes a process of authentication and validation using telephone voice calls between a precinct judge and a designated LBE official. This approach to securing the original data transfer would be subject to its own risks of social engineering, spoofing, and lack of an audit trail. The SBE has addressed the need for authentication and validation through electronic authentication and encryption protocols combined with procedural controls.

- Turn off all services and ports except for those required by GEMS.

The recommendation was implemented. The SBE received a revised list from Diebold on July 17, 2006. Pre-installation, acceptance testing and application of the new list to the LBE servers is scheduled to begin following the General Election.

- Update the anti-virus software on the GEMS Servers.

This recommendation has been implemented and is an ongoing process.

- Install Tripwire on the system to provide an audit capability on the configuration.

This recommendation has been implemented. Tripwire was recommended as a system configuration and system change audit tool. The SBE selected Maresware for audit capability rather than Tripwire.

- Disable the “autorun” feature in Windows 2000

This recommendation has been implemented.

- Ensure the front panel on the server is locked and the server is stored in a physically secure location. Apply tamper tape to the input devices and the reboot button.

This recommendation has been implemented.

- Change the boot order to make the hard drive first and password protect the BIOS to prevent changes to the boot order without physically opening the server.

This recommendation has been implemented.

- Utilize a smart card as the authentication token rather than a user name and password for loading results to the GEM Server and for accessing Gems software on the server. Communications (under SSL) between an AccuVote-TS terminal and a GEMS server must have two-sided authentication (with unique certificates) to prevent man in the middle attacks. The dial-up (PPP) authentication currently uses a password authentication protocol, we recommend a challenge-response authentication protocol.

This has not been implemented. Changing the process of uploading results vis dialup from the precincts would be a design change to the system which Diebold would need to implement and have certified.

Additionally, requiring a smart card to be used by the precinct workers to upload results on election night adds another step to the process and requires the precinct workers to keep track of another essential token. The SBE believes this increase in the complexity of uploading results introduces more risk than it mitigates.

Although the use of smart cards to control access to GEMS software on the server could be currently implemented without a design change or recertification of the system, it is unclear whether this additional step would be effective in providing additional security for the system. Ultimately the SBE employees possessing the Administrator password for the servers would need the ability to override the smart card requirement in the case of a corrupted or lost smart card.

Requiring the smart card for use when county staff log on would have little effect since the LBE system administrator is generally going to also control the custody of the smart card.

- Develop a base line configuration and audit tools to ensure compliance with the base line.

This recommendation has been implemented.

- Eliminate group accounts and establish individual user accounts on the GEMS server.

This recommendation has been implemented.

- Apply and enforce Access Control lists to the GEMS software and databases.

This recommendation has been implemented.

- Enable system auditing to record and save Access Control List events

This recommendation has been implemented.

- Digital signature of operating system and GEMS files should be calculated and securely stored off-line.

This recommendation has been implemented.

- Remove “Weighted Ballot” code from GEMS and AccuVote Touch Screens because weighted ballots are not used in Maryland elections.

This has not been implemented. This would be a design change to the system which Diebold would need to implement and have certified. It would also require creation of a unique version of the system be created for Maryland and any other states which made this a requirement.

A more desirable approach to this issue would be for Diebold to introduce an ability to disable or block the use of functionalities that are not used in a give jurisdiction. Such an ability could extend to all state specific functions of the system such as candidate rotations and straight party voting. The modification should include a method of making it easy for election officials to verify that it is correctly set.

- Establish procedures for off-line updating of all security related patches and virus definitions.

This recommendation has been implemented.

- Employ a database system with more advanced features than Microsoft Access so that the password and audit log are stored separately from the database.

This has not been implemented. This would be a design change to the system which Diebold would need to implement and have certified. We agree that the use of Access is risky and the SBE should encourage Diebold to make this change as soon as possible

- Do not allow software updates without authentication. At a minimum, demand smart card authentication to update the software on the AccuVote-TS terminal. Ideally the software should be digitally signed and verified before installation.

Maryland Procedures require and provide a structured methodology for verification of software before installation and the Ballot Station firmware is digitally signed. However, the smart card authentication has not been implemented and would be a design change to the system which Diebold would need to implement and have certified. Diebold is working on a design change to increase authentication and authorization for software uploads. That work is incomplete at this time.

- Place file protections on all the files on the PCMCIA cards.

This was completed for the Touch Screen units.

- Software integrity should be verified before and after the election to make sure no tampering has taken place. Currently there is no ability to validate AccuVote TS software after it has been loaded onto the terminal. Post election validation must be enabled.

This has been implemented for the GEMS Server. For the AccuVote TS units, the ballot station hash signature can be verified. However there is no ability to independently validate the Ballot Station software installed on a touch screen units. This is an item that Diebold is considering. However opening access to the firmware so that an independent reviewer could review, copy or perform validation routines on it provides substantial risk that the same access could be used to attack and modify the firmware. At present the firmware must be verified at installation and secure custody of the machine must be maintained. If secure custody is lost, then the firmware must be reloaded from a trusted source and secure custody reestablished. The SBE has procedures for establishing and maintaining such custody.

- Formal security training of SBE and LBE system administrators such as that provided by SANS. Server Security Templates should then be applied to GEMS Servers.

This has not been implemented as stated at this time. The RABA report is not specific as to what courses would be applicable.

We have reviewed the course listings of the SANS Institute. Their course listing is very impressive and the course descriptions appear to be very in-depth.

We agree that they are an excellent source of training that should be considered for continuing professional education by the SBE Chief Information Officer, Security Officer and System Administrators and Managers. They also provide an excellent source for LBE employees who need training to manage other IT functions of the LBE office such as office automation, web presence and management of administrative IT resources. However, we could not find a course or a reasonable combination of courses that appeared to meet the training needs of the LBE System Administrators for use with the GEMS Servers.

The LBE GEMS Server Administrator is a “Super-user” on a freestanding, isolated, and physically secured Windows 2000 server. So much of the curriculum in the SANS courses, and in courses being offered by other organizations, addresses the security issues of servers on networks with numerous client access points, and connections between the internal network and the internet.

We do agree that a structured training program should be developed for the LBE GEMS Administrators. The training should include testing or evaluation of performance to verify that the required knowledge has been transferred and that the students can correctly apply the knowledge in their offices.

Review the ISSP and Maryland's election procedure documents for security vulnerabilities or other risks to the accuracy and reliability of the system which have not been addressed

Maryland has done a good job of separating duties and incompatible functions. Normally, this is something that organizations address between employees. Maryland has built a model of separation by strategically separating duties between the State, the counties, an independent validation and verification contractor and the voting system vendor. The system is designed with the intent that no one person or one agency can do anything that is not reviewed by another person or agency and no one person or agency can control the election.

The SBE procedure for touch screen firmware acceptance and validation process is very solid. It provides a solid separation of duties between the SBE Staff, the LBE staffs, the system vendor and an independent validation and verification (IV&V) contractor. However, we found the following points where the process needs strengthening.

- The preparation of memory cards for upgrading touch screen firmware is performed by one highly trusted individual staff member of the State Board of Elections. There should be a process for some individual outside this employee's immediate span of control, perhaps the IV&V contractor, or an employee of the county, to validate the memory cards against an external source. At this point in the process, the hash value of the firmware on the distribution copy from the vendor has been taken by the SBE and verified to match the hash on file with the National Software Reference Library (NSRL). Accordingly the person conducting this external validation could use the NSRL hash as an independent benchmark for their comparison.
- The process for delivery of memory cards for upgrading touch screen firmware requires that the cards be transported in a locked and sealed bag. As the bag circulates from county to county, the county receiving it verifies that the seal numbers are the same as recorded by the sender when the bag was sealed. However, the records of seal numbers travel with the sealed bag. There should be source for the receiving official to verify that the seal number is unchanged without relying on the document which travels with the bag.
- Acceptance testing for DRE voting units does not include testing the units while they operate on battery power.

Although file protections are now in place for the files on the Touch Screen PCMCIA cards, no such protection is currently installed on the Optical Scan Units. This is a design change to the system which Diebold is currently developing but which is incomplete at this time

The documents describing the procedure for upgrading the GEMS server included no discussion of disabling extraneous services. Services which are not needed for the operation of the system should be disabled. The specific services to be disabled should be identified.

We found no standardized ballot accounting procedures for absentee ballots. The only document the State Board has is the regulations for absentee ballots. In the three counties we visited, each appears to do a good job of accounting for absentee ballots. The ballots are carefully perpetually inventoried and tracked through the canvass by the county board. However, although all three counties understood that the total absentee ballots processed and canvassed by the board must equal the total ballots tabulated, we found no procedures for verifying the count of individual batches of ballots being given to the scanner operators. An error such as some ballots not being tabulated or others being tabulated twice would ultimately be caught but, the error would not be caught at the moment it occurred, only after all ballots were tabulated. Although it is unlikely, exact offsetting errors might escape detection at the time of tabulation. The detection of such errors at the end of the process, resolving and correcting those errors, would be much more difficult than if they had been caught and corrected as soon as they occurred. The detection of such an error at the end of tabulation could possibly require that all of the ballots be rescanned.

Recommendations to mitigate unaddressed risks

We recommend that the process for installing firmware upgrades include the county staff or managers taking a Hash of the firmware to be installed and comparing that to a trusted source such as the NSRL. Both the Vendor and the State can verify that the NSRL Hash is correct and the County official can verify that the Hash of the software installed on their system matches that of the NSRL. Taking the Hash value of a file and comparing it is not difficult. County staff could easily learn to handle this task.

We recommend that the process for delivery of memory cards for upgrading touch screen firmware include independent transmission of the expected seal number on the memory card security bag by an alternate means. An e-mail or mailed memo from the administrator sealing the bag to the next administrator to receive the bag would be sufficient.

We recommend that the acceptance testing of DRE voting units include charging the machines the night before, then upgrading firmware, performing diagnostics and test voting on battery power. Any machines which began indicating a low battery during the test could be plugged back in to finish the process and their batteries serviced as necessary after the acceptance testing process is complete.

We recommend that the SBE work with the vendor to identify those services which can be disabled and include disabling those services and verification that they are disabled be included in all upgrade and maintenance procedures and scripts.

We recommend that the SBE encourage Diebold to develop upgrades to the system that will include file protection for the memory cards of Optical Scan Units.

We recommend that the SBE encourage Diebold to develop an upgrade to the system that would allow the SBE to turn off functions, such as “Weighted Ballot” elections, which Maryland does not use.

We recommend that the SBE encourage Diebold to develop an upgrade to the system that would use a database system with more advanced features than Microsoft Access.

We recommend that the SBE encourage Diebold to complete development of upgrades to the system that will increase authentication and authorization for software uploads on TS units.

We recommend that the SBE either develop, or require the LBEs to develop, processes for absentee ballots which will allow validation of the number of ballots in each batch scanned. At minimum, for each batch of ballots the scanner operator will be given the number as determined by the absentee ballot tracking or voter registration systems or by a hand count by the board. The operator will record the public count at the beginning and end of scanning the batch and will subtract the beginning number from the ending number and verify that this difference matches the number of ballots that are expected in the batch. This will ensure that any discrepancies are resolved as they are discovered.

We would recommend that the SBE consider using the services of the SANS Institute, or another equivalent provider, to developing and/or delivering a curriculum designed for the needs of the LBE GEMS Administrators.