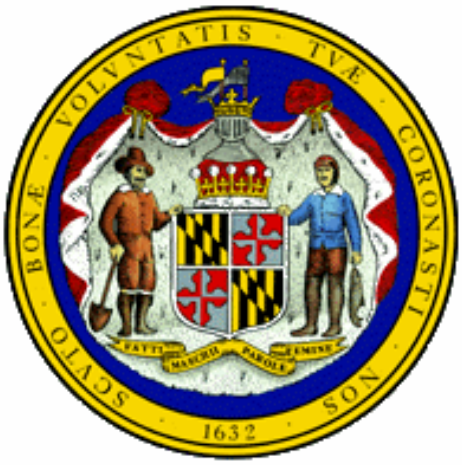

State of Maryland

State Board of Elections

Progress Report: *Department of Legislative Services' Trusted Agent Report on Diebold AccuVote-TS Voting System*

Linda H. Lamone, Administrator
Maryland State Board of Elections
151 West Street, Suite 200
Annapolis, MD 21401

Submitted: July 22, 2004

A. Introduction

In elections as in every other aspect of our lives, technology is a tool to improve processes and increase efficiencies. Maximizing the use of technology in election administration is a mandate of Maryland election law. The impact of technology in election administration has been revolutionary and, thanks in part to the leadership and assistance of the General Assembly and the Executive Department, Maryland continues to be at the forefront in election reform and the use of technology to accomplish that goal. While the benefits of technology in election administration are significant, election officials acknowledge that the introduction of technology brings additional responsibilities and requirements.

Maryland election laws and procedure contain important checks and balances to ensure the integrity of the election process, and when analyzing any voting system, it is critical to understand that a voting system includes more than just the equipment that records and tabulates the votes. It also includes the people (election officials, election judges, poll watchers), election laws, and procedures that surround and govern the election process.

The Maryland voting system has recently undergone several analyses by computer scientists and security specialists, and changes have been made to address points raised in their reports. The resultant strengthening of the electoral process should provide assurance to the public of the accuracy and security of the voting system. While it is important to recognize that these analyses were not conducted in an election day scenario that is, in a polling place under the scrutiny of election judges, poll watchers, and Maryland voters, the studies have reinforced the critical importance of the election process to our country and increased recognition of the need for security actions in all aspects of our lives. Additionally, the analyses have pointed out the need to allocate resources to protect and improve the election process.

A series of progressive security improvement measures, which include managerial, operational, and technical controls, have been applied to the voting system, and this document serves as an update to the Maryland State Board of Elections' response to the Maryland Department of Legislative Services' *Trusted Agent Report on the Diebold AccuVote-TS Voting System* (*Trusted Agent Report*). This *Progress Report* was prepared by Linda H. Lamone, State Administrator of Elections, and her staff and reflects mitigation activities performed through June 30, 2004.

This *Progress Report* contains the following sections:

A. Introduction;
B. Progress Report on the Implementation of SBE's Mitigation Strategy; and
C. Conclusion.

B. Progress Report on the Implementation of SBE's Mitigation Strategy

Explanation of the following table: **Category** and **RABA Recommendation** contain verbatim recommendations from the *Trusted Agent Report*; **SBE Mitigation Strategy** contains SBE's actions / strategies to mitigate the identified risk or threat identified in the *Trusted Agent Report*; **Status** (as of July 22, 2004) indicates SBE's current status in implementing SBE's actions / strategies to mitigate the identified risk.

Category	RABA Recommendation	SBE Mitigation Strategy	Status
Smart cards	1. Create Security Key Cards with computer-generated passwords *by precinct*. Update all the Encoders and AccuVote-TS terminals within each precinct.	▪ With over 1,600 precincts in the State of Maryland, the RABA recommendation to implement security keys *by precinct* poses a substantial risk to the efficiency and administration of the election process and could result in voters being disenfranchised. However, the risk identified by RABA has been reduced by establishing new security passwords and keys *by county* on all encoders and AccuVote-TS terminals.	County level change Completed
	2. Apply Tamper Tape to AccuVote-TS terminals to prevent non-authorized entry of Security Key Cards into the terminals.	Note: Attempts to tamper with terminals, via privacy security screen removal and unlocking of bay doors, would be quickly noticed by the diligent, trained Election Judge and others in the polling place. The Election Judge's duty is to support the apprehension of the individual for this felony criminal activity by contacting police authorities and escalating the issue via the established protocols. ▪ SBE has instructed the LBEs to apply tamper tape to the AccuVote-TS terminals and record the serial numbers during the Logic & Accuracy (L&A) tests. The LBEs are also instructed to have the Election Judges verify the serial numbers and apply new tamper tape after the units are activated on Election Day. Protocols for monitoring the tamper tape and escalating the issue if evidence of tampering is identified have been established and incorporated into Election Judge training. ▪ SBE has created the Rules of Security Behavior, instructing Election Judges on the care, control, and custody of all voting equipment.	Completed

Category	RABA Recommendation	SBE Mitigation Strategy	Status
	3. Institute strict procedures to prevent the use of unauthorized Supervisor Cards.	▪ Supervisor cards are sealed in separate envelopes and may only be accessed only by a bi-partisan pair of Chief Election Judges. ▪ To further enhance the security of the Supervisor's cards, SBE has developed physical security procedures and instructions for the LBE Election Officials and Election Judges.	Completed
AccuVote-TS Terminals	1. Secure physical access to the voting terminal. The team recommends the use of serial-number tamper tape placed both inside and outside each locked bay. This could be accomplished in the following manner: after the terminals are loaded and a zero-tape printed, the bay doors would be secured with the tamper tape and the serial numbers would be recorded. The tamper tape would need to be inspected periodically as a matter of procedure. Ultimately it would be recommended to place alarms on the bay doors.	▪ SBE has instructed the LBEs to apply the serial-numbered tamper tape over the locked bay door. SBE has developed procedures for the LBE Election Officials and Election Judges to apply the tape, record and verify the serial numbers, and inspect the AccuVote-TS terminal bay doors. ▪ Each Election Judge must read and indicate an understanding of SBE's *Rules of Security Behavior*, which instruct the Judges on proper physical security controls of the AccuVote-TS Terminals.	Completed
	2. Remove the recording software from the AccuVote-TS terminal that allows the keyboard exploit. It serves no valid function.	Note: This software is mandated by the FEC Voting System Standards. ▪ Physical security monitoring performed by the Election Judges ensures that no electronic equipment is connected to the AccuVote-TS systems. ▪ Posters warning of the consequences of tampering with voting system hardware and software were purchased and posted for the Primary and will be posted for the General Election. *Maryland Election Law Article*, Sections 16-206, 16-301, 16-801, 16-802, 16-803, and 16-804 make it a crime to tamper with voting equipment.	Completed

Category	RABA Recommendation	SBE Mitigation Strategy	Status
	3. Investigate the legal implications of tampering with the hardware systems (such as jamming the card reader and disconnecting the monitor). We see no short term fix for these attacks aside from the clear posting of rules that indicate consequences of such actions.	▪ Posters warning of the consequences of tampering with voting system hardware and software were purchased and posted for the Primary and will be posted for the General Election. *Maryland Election Law Article*, Sections 16-206, 16-301, 16-801, 16-802, 16-803, and 16-804 make it a crime to tamper with voting equipment.	Completed
GEMS Server	1. Install all known security patches from Microsoft on the GEMS servers.	Note: GEMS servers are never connected to networks that have access to the Internet, and SBE forbids connecting the GEMS servers to unprotected networks. The recommended Microsoft security patches address systems that have access to unprotected networks. ▪ SBE performed a risk assessment on Microsoft vulnerabilities and remedial patches. The risk assessment reviewed all 18 Microsoft security patches that were issued after the current operating system was installed on the GEMS server. Sixteen security patches were found not to be applicable in the SBE voting system non-networked environment. Two patches were rated as non-significant and a low risk. They are mitigated by managerial controls. ▪ Security patches that present low risk or no risk to the voting system will be tested and deployed. ▪ Future security patches will be risk assessed and deployed.	On schedule to be completed prior to November Presidential Election.

Category	RABA Recommendation	SBE Mitigation Strategy	Status
	2. Ensure modem access to GEMS is enabled *only when uploads are expected*, i.e. via voice notification over a telephone line between a precinct judge and a designated LBE official. The number used for this purpose should be *guaranteed* not to change. Validate the number being dialed and the identities of the callers. The line should remain open until both sides indicate the upload is complete. Shut off the modems when not in use.	Note: Election night results are unofficial. In accordance with established procedures, regulations and Maryland law, the tabulation of election results ("canvassing") is done in four stages: Polling Place count, First Absentee, Provisional, and Second Absentee. These four tabulations combined become the *official* election results. At each stage of tabulation, multiple checks and balances are performed by the Election Judges and county Election Officials. If unofficial election night results are modemed, the following controls have been implemented: ▪ Modem access is enabled only when the uploads are expected (i.e., election night). ▪ Modems are disengaged once uploads are completed. ▪ Strong authentication and encryption protocols are used. ▪ The LBEs that use modems on election night have been instructed by SBE to re-read 100% of the PC memory cards and compare the unofficial results received by modem with the count produced by the PC memory cards.	Completed
	3. Turn off all services and ports except those explicitly required by the GEMS software. For defense-in-depth, install firewall software to block all ports except those required by the GEMS software.	▪ The GEMS servers are never connected to the Internet or an unsecured network. ▪ SBE reviews GEMS Server security configuration. Ports and services not needed by the GEMS Server are reviewed for functionality and tested before changes are implemented.	On schedule to be completed prior to November Presidential Election.
	4. Update the anti-virus software.	▪ Anti-virus software on the GEMS servers is kept up-to-date.	Completed
	5. Turn off services that are not needed by GEMS.	▪ Services that are not needed by GEMS are reviewed and rigorously tested within the GEMS system before disengagement.	Completed
	6. Install Tripwire on the system to provide an audit capability on the configuration.	• Configuration audit control software has been evaluated and will be used on the GEMS servers. This will enable SBE to determine that no unintentional or malicious changes are introduced and go undetected.	On schedule to be completed prior to November Presidential Election.

Category	RABA Recommendation	SBE Mitigation Strategy	Status
	7. Disable the "autorun" feature in Windows 2000.	▪ SBE has implemented the recommendation.	Completed
	8. 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.	LBEs have been instructed to do the following: ▪ Ensure the GEMS servers are locked and stored in physically secure locations. ▪ Apply tamper tape to the GEMS servers. ▪ Maintain access control logs.	Completed
	9. 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.	▪ SBE will ensure the BIOS configuration is changed on each GEMS server to prevent installing unauthorized software. SBE will ensure each GEMS server has password protection applied to the BIOS configuration utility.	On schedule to be completed prior to November Presidential Election.

C. Conclusion

The November Presidential Election will be conducted in Maryland using the most secure voting system in the country. Maryland has led the nation in assessing the security of the Diebold AccuVote-TS voting system and has implemented the appropriate managerial, technical, and operational security measures that have been recommended by the assessments.

In addition to the testing performed by RABA, the source code for the voting system has been reviewed by an independent verification and validation security firm in Maryland. The Administrator has also required that the source code be held in escrow, to further protect the voting system from malicious activity.

We appreciate the identification of points where security enhancements could and have been made, and emphasize that each analysis of the source code has found that the voting system records and tabulates votes correctly. Also, since the source code has been in the public domain for over a year now, it is certainly expected that someone would have reported malicious code if it existed.

While many of the perceived threats to Maryland's electronic voting system are just that - perceived, Maryland has well prepared and vigilant election officials and Judges that are an instrumental "security safeguard". Although any electronic voting system is hypothetically "hackable," We are confident that the likelihood of this occurring is extraordinarily remote. For this to happen, there would have to be an election official collaborating and assisting with this illegal effort. Reports implying or alleging this are insulting to the dedicated and honest election officials and judges who undertake this very important civic duty.

For many voters in Maryland, this will be one of the first times they will be able to vote an unassisted, secret ballot, due to the audio capabilities of the voting system. For others, the multi-lingual and magnification capabilities will make voting much easier. All voters should appreciate the importance of these steps to give all voters a similarly satisfactory election experience.