State of Maryland

Electronic Voting System Security

Department of Budget and Management
Annapolis, Maryland
September 17, 2003

ELECTRONIC VOTING SYSTEM SECURITY

The federal Help America Vote Act requires that each state have a voting system meeting federal requirements by January 2006, including a Direct Recording Electronic (DRE) or other accessible voting unit in each precinct for voters with disabilities. Chapter 564 of the Laws of Maryland (2001) requires a uniform statewide voting system for polling places and a uniform system for absentee voting by 2006, for all jurisdictions in Maryland.

To meet these requirements the State Board of Elections (SBE) selected the Diebold AccuVote-Touch Screen for polling place voting and the Diebold AccuVote Optical Scan for absentee voting. The agency entered into a contract for the Phase I implementation covering four counties on December 12, 2001, and the system was used in those counties for the 2002 elections. SBE signed a contract modification on July 19, 2003 to provide for additional equipment and services for 19 jurisdictions (Phase II), to be used beginning with the March 2004 primary election. The remaining jurisdiction, Baltimore City, is scheduled to implement 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 Diebold touch screen voting system. The report described potential security issues and vulnerabilities of source code found on a Diebold web site and suggested that the security of the system could be compromised ~~easily~~. The report indicated that administrative controls and procedures for use of the voting system were not analyzed, and based observations on the assumption that the voting devices operate on the Internet.

In response both SBE and Diebold affirmed~~stated~~ that the devices do not operate on the Internet, and that the State's procedural controls reduce or eliminate many, if not all, of the vulnerabilities identified in the report. Nonetheless, the Rubin report, representing observations of computer security experts, prompted strong public interest in verifying security of the voting system.

On August 5, 2003, Governor Robert L. Ehrlich, Jr., directed the Department of Budget and Management to carry out an independent security review of the voting system to determine security risks, and corrective actions required to ensure the integrity of the voting process. Science Applications International Corporation (SAIC), an independent consulting firm internationally respected in the field of technology security, performed the analysis and has delivered its security analysis report.

~~The SAIC security analysis reviewed compliance with a total of 329 requirements for voting system security, including management, operational and technical controls.~~ The

analysis included testing of a complete AccuVote-TS system, software analysis, interviews of elections professionals, and reviews of administrative procedures and controls for election processing security.

A total of 329 requirements were reviewed and the following results were found: ~~A total of~~ 217 requirements (66%) were found to be met with existing procedures and technical features. ~~Forty six~~46 requirements (14%) were deemed not applicable to this specific system. ~~Sixty six~~66 requirements (20%) were found to need further action, of which 26 (8%) were judged to be high risk factors.

SAIC found few risks represented by the Diebold equipment. The most significant vulnerability, use of hard-coded passwords, has been reported by Diebold to have been corrected and submitted for federal certification. SAIC further recommended encryption of certain data in storage and in transmission, and 100% verification of data transmitted. The analysis noted that risk of compromise via the Internet is ~~minimized~~eliminated by the fact that the system is not connected to the Internet.

Risks identified were predominantly associated with a wide variety of absent administrative controls for voting system security. Among management and operational controls, SAIC found risks in the controls on access to servers, administration of passwords, use of system audit logs, intrusion detection, and level of security training for elections personnel. SAIC concluded that with the management and operational procedures currently in use, the risk of system compromise is high.

SAIC indicated however that these vulnerabilities can be mitigated, if not eliminated, by adequate security planning and administration. SBE has prepared an Action Plan in which the agency proposes to develop and carry out immediately a series of upgrades in its security procedures to meet these requirements. These include the following types of actions:

ACTION PLAN

- SBE will create and implement a formal Information System Security Plan (ISSP);
- SBE will implement a formal Information System Security Training Program;
- SBE will develop a plan for all local jurisdictions to implement policies and procedures uniformly;
- SBE will verify that no voting system server is attached to a network accessible externally.

The administrative changes are proposed to be completed in phases: Phase I by September 22, 2003; Phase II by January 31, 2004; and Phase III by March 31~~1~~, 2004.

The Board of Elections believes that:

1. Management and operational requirements can and will be met to fully assure the integrity of the voting process for all voters, including those with disabilities.

2. The Diebold AccuVote-TS system selected by the Board is capable of meeting the security requirements with minor changes and proper controls.

In considering appropriate plans, the Department of Budget and Management and SBE evaluated two main options: Continue the existing project and Diebold contract, or discontinue the contract and use an alternative voting system. Since few significant vulnerabilities were found with the Diebold equipment, which in addition meets the requirements of federal and State elections law, and since procurement of an alternative system would likely result in major costs and disruption to the election preparations in the State, continuing the present contract is recommended, subject to successful mitigation of risks identified by SAIC.

SBE proposes keeping to the original schedule of statewide implementation of the voting system by March 2004. Doing so would prevent overlap of that project with the voter registration system project, also required by 2006. An aggressive schedule is required to complete all tasks including the intensive security program by March 2004. Implementation ~~of some counties~~ by the November 2004 general election in lieu of the primary remains a possible alternative if needed. In that case, advance plans must be made with the counties to retain previously acquired equipment until the actual conversion.

SBE projects a need for three additional personnel to manage the security plan. SAIC recommended establishing one SBE System Security Officer position. Two additional State contractual positions are proposed, one to develop procedures and coordinate actions with local Boards of Election, and one to manage the voter outreach and training. SBE has received federal funds under the Help America Vote Act of 2002 (HAVA) to implement election reform, for which the Assistant Attorney General for SBE has provided an opinion that the personnel costs will be an acceptable use of funds.

The Department of Management and Budget concurs in the retention of a Systems Security Officer and the voting system vendor and contract, and recommends immediate implementation by the State Board of Elections of all security upgrades required to ensure absolute reliability and integrity of Maryland's voting process.

James C. DiPaula, Secretary

connected to a network, the risk rating would immediately be raised to high for several of the identified vulnerabilities. SAIC recommends that a new risk assessment be performed prior to the implementation of a major change to the AccuVote-TS voting system. Additionally, SAIC recommends a similar assessment to be performed at least every three years, regardless of system modification.

We recommend that SBE immediately implement the following mitigation strategies to address the identified risks with a rating of high:

- Bring the AccuVote-TS voting system into compliance with the State of Maryland Information Security Policy and Standards.
- Consider the creation of a Chief Information Systems Security Officer (CISSO) position at SBE. This individual would be responsible for the secure operations of the AccuVote-TS voting system.
- Develop a formal, documented, complete, and integrated set of standard policies and procedures. Apply these standard policies and procedures consistently through the LBEs in all jurisdictions.
- 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.
- Apply cryptographic protocols to protect transmission of vote tallies.
- Require 100 percent verification of results transmitted to the media through separate count of PCMCIA cards containing the original votes cast.
- Establish a formal process requiring the review of audit trails at both the application and operating system levels.
- Provide formal information security awareness, training, and education program appropriate to each user's level of access. -DO YOU PROVIDE TRAINING? IS IT STANDARD PRACTICE FOR THE LBE'S AND DIEBOLD TO GIVE ANSWERS TO TESTS FOR ELECTION WORKERS?
- 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 modifications, or at least every three years.
- Implement a formal, documented process to detect and respond to unauthorized transaction attempts by authorized and/or unauthorized users.
- Establish a formal, documented set of procedures describing how the general support system identifies access to the system.
- Change default passwords and passwords printed in documentation immediately.

- Verify through established procedures that the ITA-certified version of software and firmware is loaded prior to product implementation.

- Remove the SBE GEMS server immediately from any network connections. Rebuild the server from trusted media to assure and validate that the system has not been compromised. Remove all extraneous software not required for AccuVote-TS operation. Move the server to a secure location.

- Modify procedures for the Logic and Accuracy (L&A) testing to include testing of time-oriented exploits (e.g., trojans). This may be accomplished by changing the machine date and time to correspond to that of the election during testing.

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

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

The system, as implemented in policy, procedure, and technology, is at high risk of compromise. Application of the listed mitigations will reduce the risk to the system. Any computerized voting system implemented using the present set of policies and procedures would require these same mitigations.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

1.1. Overview

The State of Maryland has contracted with Science Applications International Corporation (SAIC) to perform a risk assessment of the Diebold AccuVote-TS voting system as currently implemented at the State and County levels.

The risk assessment was performed from August 5, 2003 through August 26, 2003. This risk assessment was conducted during the operational phase of AccuVote-TS life cycle. If major changes are made to AccuVote-TS after completion of this risk assessment, then the findings of this assessment should be revisited using the same formal methodology. In addition, the AccuVote-TS risk assessment should be updated at least every three years or following major system changes or security incidents in accordance with State of Maryland requirements.

1.2. Purpose

The purpose of this risk assessment report is to describe the results of applying a tested risk assessment methodology to the AccuVote-TS voting system, as currently implemented at the State and County levels. This report is intended to be a stand-alone document and contains the following information:

- A description of the methodology and approach used to conduct the risk assessment.
- A description of the relevant aspects of the AccuVote-TS voting system including functionality, architecture, connectivity, procedures, and security controls.
- The findings that resulted from performance of the risk assessment. The report includes the applicable State Board of Elections (SBE) security requirements; description of security controls; identification of threats, vulnerabilities, threat likelihood; an impact analysis; and finally recommendations to mitigate the unmet SBE security requirements.

1.3. Scope

This risk assessment was performed using the methodology documented in National Institute of Science and Technology (NIST) SP 800-30, *Risk Management Guide for Information Technology Systems,* and in the State of Maryland's Certification and Accreditation Guidelines. This assessment consists of agency-directed, independent verification of systems, software, and processes associated with the system. This assessment provides an in-depth analysis of security controls, including comprehensive personnel interviews, documentation reviews, site surveys,

and evaluation of the system's hardware and software. Overall, this assessment measures the level of assurance that the security controls for the system are correctly implemented and are effective in their application.

1.4. Document Organization

This Risk Assessment Report is organized as follows:

- Section 1 provides an overview of the AccuVote-TS risk assessment including the background, purpose, and scope.
- Section 2 provides a summary of the risk assessment results, including possible mitigation strategies. This section also provides a high-level response to the comments made in the Rubin Report of July 23, 2003.
- Section 3 documents the methodology and approach used to perform this risk assessment.
- Section 4 provides a description of the AccuVote-TS in terms of functionality, architecture, connectivity, and procedures with an emphasis on the security features of the implementation of the AccuVote-TS.
- Section 5 provides the risk assessment findings, including a discussion of SBE security requirements, threats to the implementation of the AccuVote-TS, likelihood of exploitation of the threat, vulnerabilities, and mitigation strategies and recommendations for improving the security posture.
- Appendix A contains a listing of the acronyms used in this report.
- Appendix B contains a matrix of the security statements from the Aviel D. Rubin analysis of some Diebold code entitled, "Analysis of an Electronic Voting System", dated July 23, 2003. The matrix references the page number from Mr. Rubin's report, the actual security statement, the SBE security requirement reference, and any existing controls that address the statement.
- Appendix C contains a listing of interviews conducted by SAIC in the course of this assessment.
- Appendix D contains a listing of documents reviewed in the course of this risk assessment.

2. MAJOR RISKS AND MITIGATION STRATEGIES

During this risk assessment, SAIC has identified several high-risk vulnerabilities that, if exploited, could have significant impact upon the AccuVote-TS voting system operation. In addition, successful exploitation of these vulnerabilities could cause damage to the reputation and interests of the State Board of Elections (SBE) and the Local Boards of Elections (LBE). Also identified in this risk assessment are numerous vulnerabilities with a risk rating of medium and low. ~~Tables 5.1 through 5.3 provide a high-level summary of the management, operational, and technical controls currently implemented. Table 5.8 provides a detailed analysis of the vulnerabilities and suggested mitigating strategies.~~

This section provides a summary of the identified high-risk items in Sections 2.1, 2.2, and 2.3. Section 2.4 provides a summary of the review of the Rubin Report findings. In order to ensure the integrity of the AccuVote-TS voting system, all of the risks identified within this risk assessment should be considered. This assessment of the security controls within the AccuVote-TS voting system is dependent upon the system being isolated from any network connections. If any of the AccuVote-TS voting system components, as presently configured and architected, were connected to a network, the risk rating would immediately be raised to high for several of the identified vulnerabilities within this risk assessment. SAIC recommends that a new risk assessment be performed prior to the implementation of any major change to the AccuVote-TS voting system, and at least every three years.

2.1. Management Controls

2.1.1. AccuVote-TS voting system is not compliant with State of Maryland Information Security Policy & Standards

All Information Technology (IT) systems must be compliant with the State of Maryland Information Security Policy and Standards. The AccuVote-TS voting system does not meet all of these requirements.

Failure to meet the minimum security requirements set forth in the State of Maryland Information Security Policy and Standards indicates that the system is vulnerable to exploitation. ~~The results of a successful attack could result in voting results being released too soon, altered, or destroyed. The impact of exploitation could lead to a failure of the elections process by failing to elect to office, or decide in a ballot measure, according to the will of the people. The impact could be a loss of voter confidence, embarrassment to the State, or release of incomplete or inaccurate election results to the media.~~

SAIC recommends that the SBE and the LBEs implement the mitigation strategies detailed in this Risk Assessment to bring the AccuVote-TS voting system into compliance with the State of Maryland Information Security Policy and Standards. To facilitate this compliance, we further recommend that the State consider the creation of a Chief Information Systems Security Officer (CISSO) position at SBE. This individual would be responsible for the secure operations of the AccuVote-TS voting system.

2.1.2. SBE has not ensured the integrity of the AccuVote-TS voting system

The State of Maryland and SBE have begun a process to ensure the integrity of the AccuVote-TS voting system as evidenced by initiating this Risk Assessment. In addition, the SBE and the LBE have established procedures for the AccuVote-TS voting system. However, these controls are neither complete, nor integrated.

~~Failure to ensure the integrity of the AccuVote-TS system could result in vital information being changed such that this information no longer accurately reflects the collective will of the voters.~~

We recommend that the SBE and the LBEs immediately implement the mitigation strategies detailed in this Risk Assessment for all "high" risk ratings. The SBE should create a formal, documented, complete, and integrated set of policies and procedures. These policies and procedures should be applied consistently by the LBE in each jurisdiction. In addition, the SBE should implement an iterative process to ensure that the integrity of the AccuVote-TS voting system is maintained throughout the life cycle process.

2.1.3. SBE has not created a System Security Plan

Currently, no formal documented System Security Plan exists for the AccuVote-TS voting system. The purpose of a System Security Plan is to provide an overview of the security requirements of the system and describe the controls in place or planned.

The absence of this plan could result in security controls have been missed, or if considered, implemented incompletely or incorrectly. ~~Exploitation of any of the resultant security holes could lead to voting results being released too soon, altered, or destroyed. The impact of exploitation could lead to a failure of the elections process by failing to elect to office, or decide in a ballot measure, according to the will of the people. The impact could be a loss of voter confidence, embarrassment to the State, or release of incomplete or inaccurate election results to the media.~~

We recommend that the SBE develop and document 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.

2.1.4. SBE does not require the secure transmission of election vote totals

The SBE does not require encryption for the election results transmitted from the local polling sites to the LBE. ~~These results are transmitted over a private, point-to-point connection, via modem. These transmitted results become the official results after the canvassing process is completed. A 100% verification of the transmitted totals to the original PCMCIA cards (i.e., computer memory storage of actual vote totals) or the paper totals is not performed.~~

~~Unencrypted information could be intercepted and released prematurely, or altered. Since the transmissions do not undergo a 100% verification it is possible that an alteration of voting results would go undetected.~~

We recommend that SBE require the implementation of cryptographic protocols for the protection of the transmissions. In addition, we recommend a 100% verification of transmitted results to the PCMCIA cards. Based upon our interviews with the LBEs, the time required to reload the PCMCIA cards for 100% verification of the transmissions at the LBE would not be significant.

2.1.5. SBE does not require the review of the computer audit trails

~~SBE has no documentation requiring the review of audit trails, the description of audit trail configurations, or requirements of the events to be audited at either the application or operating system levels.~~

~~Failure to regularly review audit logs allows improper system use to go undetected, perhaps indefinitely.~~

We recommend that SBE document a formal process requiring the review of audit trails at both the application and operating system levels. In addition, the process should detail which events should be audited, configuration of the audit trails, and frequency of review.

2.1.6. The AccuVote-TS voting system training does not include an information security component

The training materials for the AccuVote-TS voting system do not include an information security component. The increasing number of threats to IT systems has resulted in the need for security awareness, training, and education at all levels.

Failure to conduct security awareness, training and education leaves election officials at all levels potentially unaware of the vulnerabilities and threats to their system. Without this awareness, the officials may not correctly or completely carry out vital security duties. Since the security of the

AccuVote-TS system relies on non-technical controls performed by personnel, such as election judges, this awareness is vital to ensuring the security of the system.

We recommend that SBE document and implement a formal information security awareness, training, and education program appropriate to each user's level of access.

2.1.7. SBE does not require a review of security controls after significant modifications are made to the AccuVote-TS voting system

SBE does not have a formal risk assessment process for reviewing the impact of significant system modifications to the security controls for the AccuVote-TS voting system. Results from this risk assessment will serve as a baseline to determine the effectiveness of existing security controls and to provide recommendations for security deficiencies.

In the absence of a formal process, SBE cannot ensure that the security controls remain effective. Any system change could affect the level of risk to the system. Even without system changes, the changing technology and environment that surround the system can cause the risk profile to be significantly altered.

We recommend that all system modifications be reviewed through a formal, documented change control process to ensure that the changes do not negate any security controls that are currently in place. In addition, a risk assessment should be performed any time a major system modification is performed, or at least every three years regardless of change status.

REDACTED

2.1.8. ~~Controls are not implemented to detect~~ Unauthorized transaction attempts by authorized and/or unauthorized users

~~There is no documentation that describes security controls for detecting unauthorized transaction attempts by authorized or unauthorized users. Therefore, the application of security controls may be applied inconsistently, incorrectly, or incompletely.~~

Since a threat source is more likely to exploit a system if the evidence of his/her actions cannot be gathered or will go undetected, failure to have controls for detection increases the likelihood of system attacks, and consequently, of system compromise.

We recommend that a formal, documented process be implemented to detect unauthorized transaction attempts by authorized or unauthorized users. This process would include the review of audit logs cited in paragraph 2.1.5.~~, but could also include installation of host based intrusion detection systems on the GEMS servers. The GEMS server at the SBE headquarters is particularly susceptible to misuse as discussed in paragraph 2.2.2, 2.3.1, 2.3.2 and 2.3.3.~~

2.1.9. No documentation currently exists regarding appropriate access controls to the AccuVote-TS voting system

There is no documentation that identifies the process for maintaining appropriate access controls to the AccuVote-TS voting system. Without proper documentation, the consistent implementation of security controls cannot be verified or validated.

~~The lack of proper documentation has resulted in the vendor default settings being left in place with the default user ID in the configurations. This information (i.e., passwords) is also documented in various manuals.~~

~~Failure to correctly document access procedures, and use of vendor, default passwords allows anyone with access to those documented passwords authenticated user privileges to the system. That access would allow the unauthorized user to do anything the legitimate user could do.~~

We recommend that a formal, documented set of procedures be implemented that describe how the general support system identifies access to the system, specifically, unique identification, correlation of user actions, maintenance of user IDs and inactive user IDs. ~~In addition, we recommend that all passwords be removed from the various existing documents and be changed immediately. Subsequently, the documented procedures should ensure that all future documentation is free of system passwords.~~

2.2. Operational Controls

2.2.1. SBE relies upon Diebold (the AccuVote-TS vendor) to load the version of software certified by the Independent Test Authority (ITA)

The SBE is required to ensure that the implemented software version and firmware version of the AccuVote-TS is the one certified by the ITA. The SBE relies upon Diebold to load the certified versions, therefore Diebold could load uncertified versions. Diebold has a contractual obligation to load only the ITA-certified versions, but controls are not in place to ensure that this occurs. ~~An uncertified version may contain malicious code, or untested code that could result in the loss of confidentiality, integrity, and/or availability of the AccuVote-TS voting system.~~

We recommend that SBE establish and implement procedures to verify that the ITA certified version of software and firmware is loaded prior to production implementation.

2.2.2. SBE GEMS server is connected to the SBE intranet

The current security controls employed for the AccuVote-TS voting system require that the system not be connected to any network. The Direct Recording Equipment (DRE) voting

terminals themselves are not connected to any network. However, the SBE Global Election Management System (GEMS) server is connected to the SBE intranet, which has access to the Internet. In addition, the server contains some Microsoft Office products not required for the operation of the AccuVote-TS voting system. ~~The server is located in an open office.~~

~~The SBE GEMS server is used to generate and distribute ballots. The approved ballots are transferred from the SBE GEMS server to an FTP server where they are retrieved by the LBEs. The LBEs conduct proofing and Logic and Accuracy (L&A) testing prior to elections. However, the Logic and Accuracy testing does not check for time-triggered exploits (e.g., trojans) that could modify the ballot with time-triggered malicious code.~~

~~We recommend including testing for time-triggered exploits (e.g., trojans) as a part of the L&A testing. If L&A testing proves to be an inappropriate venue for this testing, we recommend the SBE choose another venue, or introduce into the testing protocol an additional battery of tests including these procedures.~~

We recommend that the SBE GEMS server be immediately removed from any network connections. The server should be rebuilt from trusted media to assure and validate that the system has not been compromised. ~~All extraneous software and subsequent open port connections not required for the AccuVote-TS operation should be removed and the server should be placed in a secure location.~~

We recommend that SBE discontinues the use of an FTP server to distribute the approved ballots.

2.3. Technical Controls

2.3.1. Audit logs are not configured properly, and are not reviewed

~~The GEMS server audit logs are not configured to log any security events (i.e., extended logging) at the operating system level and the current log size is too small. Consequently, recorded events are overwritten. In addition, the audit logs are not reviewed.~~

Failure to properly log, and to review those logs makes it significantly more likely that an intruder's actions will not be detected. Assurance of non-detection may encourage a possible intruder to attempt a penetration of the system.

We recommend that the ~~Windows 2000~~ operating system be configured to audit all security events and the log size should be set to an appropriate size. We also recommend that the event logs be reviewed on a regular basis.

2.3.2. GEMS server configuration is not compliant with State of Maryland Information Security Policy & Standards for identification and authentication

~~System account IDs with administrator privileges are shared and passwords are not compliant with the State of Maryland Information Security Policy and Standards. Unique user IDs are required to establish individual accountability.~~

~~Without this accountability, it is impossible to know who performed any given act on the system.~~

We recommend that the GEMS servers be configured to comply with the State of Maryland Information Security Policy and Standards for identification and authentication. The State of Maryland Information Security Policy and Standards require each user to have a unique user ID and password. ~~Passwords must meet requirements for length and complexity. State policy farther requires that passwords not be shared. Default passwords are required to be changed at first log in.~~

~~GEMS server user session never times out and allows unlimited password guessing~~

~~The GEMS server does not lock user accounts after a period of inactivity, and the server allows unlimited authentication attempts, providing the potential for password guessing.~~

~~Failure to use locking screens or session time outs allows users to leave terminals unattended for extended periods, without the system requiring password authentication for reentry. Anyone with physical access to the server could use the server, as if they were the authorized user.~~

~~Allowing infinite password attempts allows an attacker to employ password guessing strategies or brute force password cracking utilities without the system preventing access.~~

~~We recommend that the GEMS servers be configured to comply with the State of Maryland Information Security Policy and Standards for session time outs, password age, and failed logon attempts.~~

2.4. Review of Rubin Report

In the course of this risk assessment, we reviewed the statements that were made by Aviel. D. Rubin, professor at Johns Hopkins University, in his report dated July 23, 2003. While many of the statements made by Mr. Rubin were technically correct, it is clear that Mr. Rubin did not have a complete understanding of the State of Maryland's implementation of the AccuVote-TS voting system, and the election process controls in general. It must be noted that Mr. Rubin states this fact several times in his report and he further identifies the assumptions that he used to reach his conclusions.

In general, most of Mr. Rubin's findings are not relevant to the State of Maryland's implementation of the AccuVote-TS system because the voting terminals are not connected to a network. In addition, LBE procedures and the openness of the DRE voting booth mitigate a large portion of his remaining findings.

We do concur with Mr. Rubin's assessment that if the AccuVote-TS voting system were connected to a network that several high-risk vulnerabilities would be introduced. We also concur with Mr. Rubin's assessment that transmissions of data are not encrypted in transit, and we have recommended that this be rectified.

The State of Maryland procedural controls and general voting environment reduce or eliminate many of the vulnerabilities identified in the Rubin report. However, these controls, while sufficient to help mitigate the weaknesses identified in the July 23 report, do not, in many cases meet the standard of best practice or the State of Maryland Security Policy.

2.5. Overall Risk Rating

The system, as implemented in policy, procedure, and technology, is at high risk of compromise. Application of the listed mitigations will reduce the risk to the system. Any computerized voting system implemented using the present set of policies and procedures would require these same mitigations.

3. RISK ASSESSMENT METHODOLOGY AND APPROACH

The following sections document the nine-step risk assessment methodology, in accordance with NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, and in the State of Maryland's Certification and Accreditation Guidelines, that was used as the basis for this Risk Assessment report. Additionally, the approach takes into account a combination of assumptions regarding the security controls within State of Maryland that have an impact on the security of the AccuVote-TS voting system.

3.1. Assumptions

This Risk Assessment report and its findings are based on the following assumptions:

- The system risks discussed in this report are based on the AccuVote-TS functional description. Changes to data flow, data control, data storage, software configuration, hardware configuration, networking, or system interfaces could significantly alter system risks.
- The opinions and recommendations contained in this Report are dependant on the accuracy, completeness and correctness of the data, specifications, documents and other information provided by the State of Maryland, whether provided in writing or orally.
- The equipment, documentation, and materials deployed for use by the State of Maryland will have the same configuration as that provided to SAIC for this examination.
- Based on customer direction and time constraints, this Risk Assessment is limited to the examination of human threat sources; natural and environmental threats are outside of the scope of examination.
- The process for the initial ballot creation, which occurs prior to entering into GEMS, is outside of the scope of this examination.
- The process for determining voter eligibility is outside of the scope of this examination.
- This risk assessment did not assess previous elections or implementations of this system.
- The Independent Testing Authority (ITA) complies with the standards set forth by the Federal Election Commission (FEC) for voting system evaluation and certification.
- The processes and procedures used by the Counties reviewed for conducting elections using the AccuVote-TS are representative of the overall process.
- This Risk Assessment Report captures threats, vulnerabilities, risks and suggested mitigation strategies as they exist at the publication of this report. Changes in technology could significantly alter the system's security, even if the system itself does not change.

- SAIC cannot guarantee or assure that risks, vulnerabilities and threats other than those addressed in this report will not occur nor can we guarantee or assure that, even if the State of Maryland implements the recommendations we have proposed, the State's business, facilities, computer networks and systems, software, computer hardware and other tangible equipment and assets will not be compromised, damaged or destroyed.

~~This report is for the internal use of the State of Maryland and should not be distributed outside the State's protected channels. Doing so will significantly increase the State's risk.~~

3.2. Methodology and Approach

The SAIC team, consisting of staff with expertise in management, operational and technical information technology (IT) security, conducted the risk assessment of the AccuVote-TS voting system. The SAIC team applied the nine-step risk assessment methodology, as depicted in Figure 3-1, to perform the risk assessment.

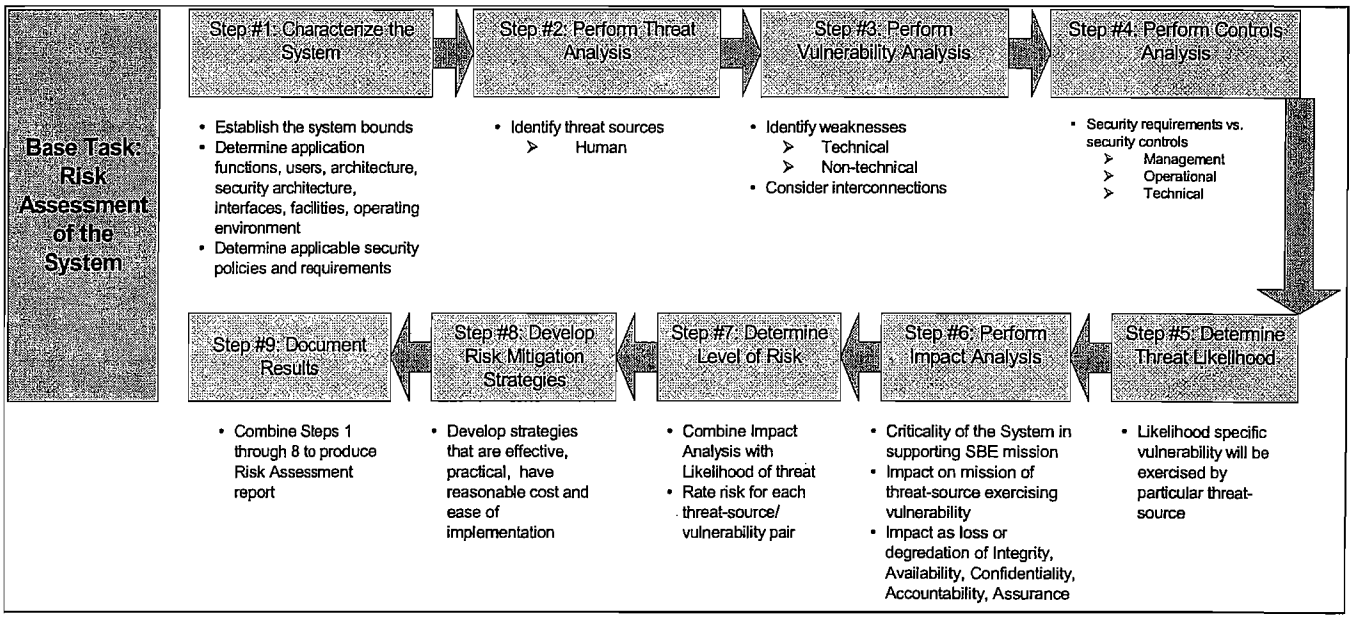


Figure 3-1: Risk Assessment Methodology and Approach

The following sections define the nine-step methodology used to complete the risk assessment for the AccuVote-TS.

3.2.1. Step 1: Characterize the AccuVote-TS Voting System

Step 1 consists of defining the system for the risk assessment. During this step the key system elements, such as hardware, software, system interfaces, data and information, personnel actions, and the mission of the AccuVote-TS voting system, are reviewed. The application boundaries,

application criticality, data sensitivity, and functional systems description are developed from the examination of the specific components as described below.

Establish System Bounds. System bounds establish the scope of the risk assessment. Clearly defined security boundaries of the system are established and approved by the State of Maryland. Within the established security boundaries, security domains are determined based on system functionality and purpose.

Determine Application Functions, Users, Architecture, Security Architecture, Interfaces, and Operating Environment. The system's function is determined and essential elements are identified during this step. Network diagrams and architectural drawings were provided to the risk assessment team.

Determine Applicable Security Policies and Requirements. Applicable security policies and requirements, in addition to any existing policies, procedures, or standards that affect AccuVote-TS security must be determined during this process. Results of previous risk assessments, audits, and certifications, and application related documentation are collected and reviewed by the SAIC risk assessment team in concert with State and County representatives.

3.2.2. Step 2: Perform Threat Identification

Step 2 consists of determining the threats posed to the AccuVote-TS voting system. Key elements, such as previous attacks on the AccuVote-TS and data from IT security-related organizations, will be examined for applicability to the AccuVote-TS.

Identify Threat Sources. Human threats to the AccuVote-TS voting system will be identified and documented by the SAIC team.

3.2.3. Step 3: Perform Vulnerability Identification

In Step 3, the vulnerabilities of the system will be examined and identified. Results from prior audits, tests, inspections, and an examination of the current state of the AccuVote-TS voting system are used to determine existing weaknesses as described below.

Identify Weaknesses. A comprehensive review of the security configurations, policy standards, procedures, and degree of compliance of both technical and non-technical requirements will determine areas where the AccuVote-TS voting system is vulnerable.

Consider Interconnections. In addition to identifying weaknesses in the above, external entities and their connectivity to the AccuVote-TS voting system will be reviewed.

3.2.4. Step 4: Perform Controls Analysis

This step examines the security controls and mechanisms for the AccuVote-TS voting system as currently implemented. Controls analysis involves examining the system security requirements and the security controls employed by the system.

Security Requirements versus Security Controls. The management, operational, and technical controls are examined to determine the degree of compliance with established security requirements and the degree of protection to data confidentiality, integrity, and availability.

Consider Controls Employed by the AccuVote-TS voting system. Security controls and mechanisms for the AccuVote-TS voting system are checked systematically against applicable security requirements. Table 5.8 presents the requirements matrix, identifies AccuVote-TS voting system compliance, and presents a rationale for the compliance/non-compliance rating.

3.2.5. Step 5: Determine Threat Likelihood

This step is based on the results of the threat identified in Step 2, and includes examination of that threat against each vulnerability to arrive at a likelihood rating of High, Medium, or Low.

Likelihood Specific Vulnerability will be Exercised by Particular Threat. The threat sources identified in Step 2 are examined against the nature of the threat and the security controls in place to counter the threat. In the case of the human threat, motivation and capabilities are taken into account as well.

3.2.6. Step 6: Perform Impact Analysis

Step 6 is used to determine the probable result of a successful exploitation of a vulnerability or weakness by a threat. This risk assessment is used to determine impact on the AccuVote-TS voting system if vulnerabilities are successfully exploited. The process used to evaluate the impact of a successful exploitation of a given vulnerability is discussed below.

Criticality of the AccuVote-TS voting system in Supporting State of Maryland Mission. The critically of the AccuVote-TS voting system to the State of Maryland mission is viewed in the scope of a successful exploitation attempt.

Impact on Mission of Threat source Exercising Vulnerability. The probable impact of a successful exploitation of the AccuVote-TS voting system is determined in this sub-step.

Impact as Loss or Degradation of Integrity, Availability, Confidentiality, Accountability, or Assurance. The effects on the AccuVote-TS voting system of the successful exploitation of a vulnerability is analyzed as to its effectiveness in modification/destruction of data, loss of service, loss of public trust, or embarrassment to the State of Maryland.

3.2.7. Step 7: Determine Level of Risk

Step 7 provides a total risk rating for each vulnerability by combining the results of the Impact Analysis established in step 6 with Likelihood of Threat established in step 5. The combination of the impact analysis and the threat likelihood versus the security controls in place is applied to a risk-level matrix to determine the resultant risk-level.

Rate Risk of each Threat-Source/Vulnerability Pair. Each Threat-Source/Vulnerability is assigned a rating of High, Medium, or Low.

3.2.8. Step 8: Develop Risk Mitigation Strategies

Step 8 seeks to provide solutions to the risks identified and quantified in the previous step.

Develop Risk Mitigation Strategies that Are Effective, Practical, Have Reasonable Cost and Ease of Implementation. Countermeasures or risk-mitigation strategies are developed. When several strategies are apparent, they are categorized from most effective, least cost, and easiest implementation.

3.2.9. Step 9: Document Results

The objective of step 9 is to *Combine Steps 1 through 8 to Produce a Final Risk Assessment Report.* The results of steps 1 through 8 are combined into a comprehensive report.

4. ACCUVOTE-TS CHARACTERIZATION, STEP 1

This section describes the AccuVote-TS voting system as required in Step 1 of the NIST SP 800-30, *Risk Management Guide for Information Technology Systems* and in the State of Maryland's Certification and Accreditation Guidelines.

4.1. Functional Description of the AccuVote-TS

The State of Maryland is implementing a statewide electronic voting system, Diebold's AccuVote-TS. SBE's Mission Statement includes:

"...to standardize voting in the State on an electronic voting system while providing increased accessibility to the process for the State's voting populace."

The statewide implementation will standardize voting processes for 24 jurisdictions. The implementation is broken into three phases with estimated completion of third phase being 2006.

Purpose and function of the AccuVote-TS voting system:

- Generate electronic ballots;
- Permit voters to view and cast their votes electronically;
- Record, store, and report vote totals; and
- Provide accurate electronic audit trails to ensure integrity of the AccuVote-TS voting system.

Figure 4-1 is a high-level diagram showing the infrastructure and connectivity for the AccuVote-TS application.

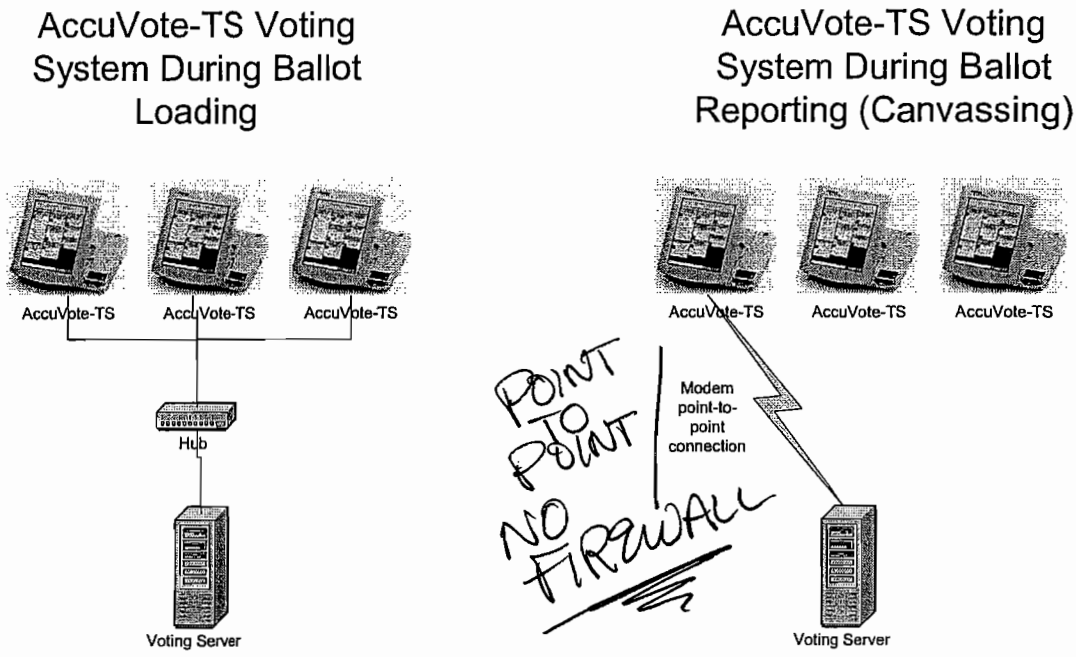


Figure 4-1: AccuVote-TS High-Level Infrastructure and Connectivity

4.2. AccuVote-TS System and Interfaces

The Diebold AccuVote-TS voting system consists of two components, the GEMS voting server and the DRE (Direct Record Entry) or voting terminal.

The voting terminal is an embedded device running Microsoft Windows ~~CE 3.0~~ as its operating system. The currently used version of the AccuVote-TS software is ~~4.3.1.5, and is~~ written in the C++ language. The components of the system include: a touch screen, used by voters for entering votes; an active memory component which stores the operating system, ballot information and a temporary record of the votes; a PCMCIA flash memory card which also stores the votes cast (this card is contained in a locked compartment on the DRE device, but is removed for vote tallying); And an internal ribbon printer. The system also has an optional audio component, which can be activated to support the visually impaired. Each of the systems is able to support a modem.

~~The GEMS voting server is a Dell PowerEdge server running Microsoft Windows 2000 Server with Service Pack 3.~~ The GEMS voting server contains the GEMS software, which is used to communicate with the voting terminals for loading ballots and transferring the voting results. The currently used version of the GEMS software ~~is 1.18.18 and~~ is also written in C++. The components of the system include the server, a keyboard, mouse and monitor. The server can be connected to a modem bank to receive voting information from the precincts. Each LBE has two GEMS voting servers, a primary and a back-up. The LBE voting server and terminal are

connected to a non-public network during the ballot loading process. The only other instance when the LBE GEMS voting server and terminal are connected is during the results collection or canvassing stage. ~~At that time, the LBE GEMS voting server and terminal are connected using a modem point-to-point connection.~~ All other times, the voting terminal operates in a stand-alone mode.

~~SBE also has a GEMS server. The SBE GEMS server is located at SBE headquarters on 151 West Street, Annapolis, MD. This server is permanently connected to the SBE intranet. This server is used to prepare the electronic ballots and for the tallying of votes. The electronic ballots are prepared and then loaded to a FTP site where the ballots are downloaded by the LBE for the local jurisdiction. For vote tallying, each LBE emails their composite vote tally in the GEMS file format to SBE. The LBE also performs a screen print of their composite vote tally that is printed and faxed to SBE. The LBE also uploads the composite vote tally to the FTP site where it is retrieved by SBE and reconciled with the email and fax.~~

4.3. System Users

This subsection identifies the types of users that are authorized to use the AccuVote-TS system.

4.3.1. Internal Users

Internal privileged users of the AccuVote-TS system are required to logon to the GEMS voting server to perform operations to the ballot or to communicate with the voting terminals. The accounts are password protected, but the accounts are shared among users, which does not provide accountability.

Internal privileged users, such as election judges, have direct access to the DRE voting terminals. The election judge has a supervisor smartcard, which is used to start and close elections. Starting and closing elections requires the use of the supervisor smartcard, and a PIN number.

4.3.2. External Users

External users have direct access only to the DRE voting terminals, and are limited to eligible voters. The eligible voter is given a one-time use smartcard by the election official to enable the voter to vote. Once their ballot has been cast, the smartcard is disabled until it is re-enabled for use by a new voter by the election official. The smartcards do not contain any sensitive data.

The voting process is as follows. The local election officials verify a voter's eligibility to vote. Once confirmed as an eligible voter, the local election judges have the voter verify the information on his or her Voter Authority Card (VAC), make necessary changes, sign the VAC and instruct the voter on taking the signed VAC to the next step in the voting process. The VAC card is a paper card that contains information about the voter. These VAC cards are used to verify the vote totals at the conclusion of the election against the vote totals stored in the DRE memory.

The next step in the voting process is for the voter to present his or her VAC to the election official responsible for the DRE voting terminal. The election official takes the voter's VAC and activates a DRE Voter Access Card smartcard for that voter. The election official places the voter's VAC in the envelope associated with the DRE terminal and permits the voter to insert the DRE Voter Access Card smartcard into the DRE to vote.

4.3.3. Special Processing IDs

There are no special processing IDs for the AccuVote-TS system.

FROM HERE ON - COMPLETELY REDACTED

~~5.RISK ASSESSMENT RESULTS, STEPS 2-9~~

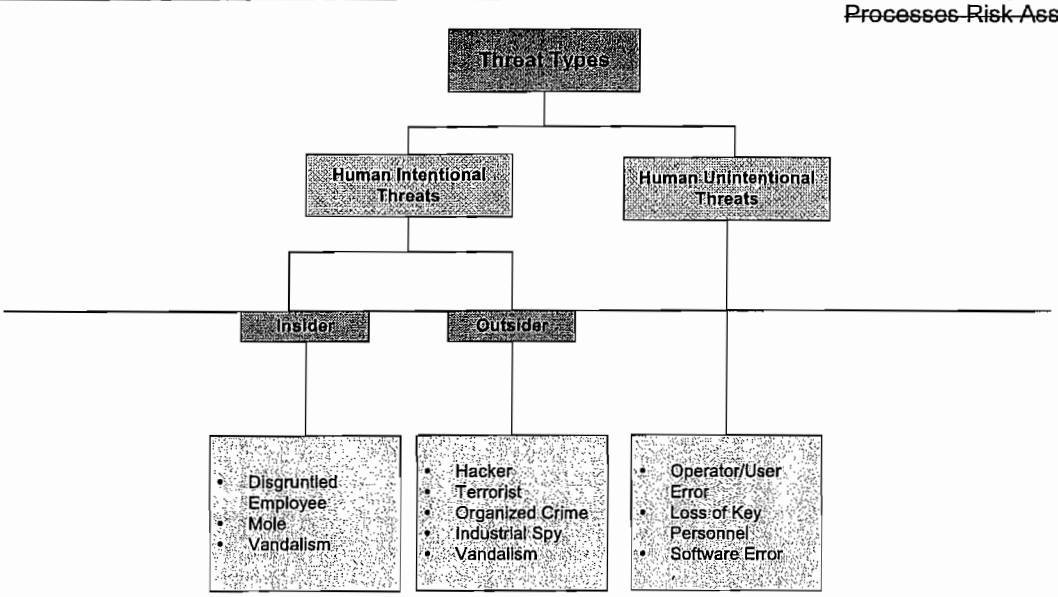
~~This section provides the findings of the risk assessment, following Steps 2 through 9 of the risk assessment methodology. The results are provided in tabular form. Each of the vulnerabilities is:~~

- ~~Matched to a threat source.~~
- ~~Evaluated for likelihood of exercise rating along with a rationale for the rating.~~
- ~~Analyzed to determine the impact rating if the vulnerability is exercised.~~
- ~~Assigned a risk rating that is determined by multiplying the likelihood rating by the impact rating.~~

~~5.1.Step 2 – Threat Identification~~

~~Security threats can lead to loss of or damage to the AccuVote-TS voting system components, or the inability to provide data confidentiality, integrity and availability for the AccuVote-TS voting system. Threat exploitation could result in SBE being unable to accomplish its mission in a timely manner. Vulnerabilities that result from unmet security requirements could be exploited, resulting in realized threats. Both the source and the nature of possible threats must be understood in order to attempt to prevent the threat from occurring. Human threats may be present within the State of Maryland personnel in the form of an authorized user who has a valid user ID and password. Alternatively, the threat may be from outside the State of Maryland personnel as represented by an unauthorized (malicious threat source) with malicious intent. It is prudent to assume that where vulnerabilities exist there is the possibility the vulnerability will be exploited.~~

~~The State of Maryland and the SAIC Risk Assessment Team have identified two broad categories of human threat sources applicable to the AccuVote-TS voting system; other threat sources are outside the scope of this Risk Assessment. Figure 5-1 shows the two broad human threat source categories and lists the set of specific threat sources that could exploit AccuVote-TS vulnerabilities.~~



~~Figure 5-1: State of Maryland Threat Sources~~

~~5.2.Step 3 – Vulnerability Identification~~

~~The AccuVote-TS voting system vulnerabilities were examined at the State of Maryland Department of Budget and Management (DBM) at 45 Calvert Street in Annapolis, MD.~~

~~The vulnerabilities were identified through a combination of reviews of documented policies and procedures and interviews of State and County officials, in conjunction with a review of the hardware and software components of the AccuVote-TS voting system. The identified vulnerabilities are presented in Table 5-8.~~

~~5.3.Step 4 – Controls Analysis~~

~~This section links the principles of the three control areas: (1) management, (2) operational, and (3) technical, with the status of AccuVote-TS voting system compliance and implementation. These three types of controls are normally used in combination to prevent, limit, deter, or detect damage to the AccuVote-TS voting system and the SBE mission.~~

~~Tables 5-1 through 5-3 list core principles of required management, operational and technical security controls. Each principle is coupled with an analysis of the AccuVote-TS voting system compliance status, including planned implementations where necessary.~~

~~5.3.1.Management Controls Analysis~~

~~Management controls address core or fundamental principles that are inherent in the protection of information systems to manage risk.~~

Table 5-1: Management Controls

Management Controls	
Principle	**AccuVote-TS Implementation**
Separation of duties: The primary purpose is to prevent and properly detect errors in the IT system. No one individual or like group of individuals should have full control of the administration and security monitoring of the IT system. Duties are considered incompatible if someone can carry out and conceal an action in the course of day-to-day activities.	The SBE and LBEs have implemented separation of duties where feasible. Given the limited number of individuals responsible for maintaining the AccuVote-TS voting system, individuals are often tasked with multiple assignments and responsibilities.
Policies and procedures: Standard polices and procedures provide guidance in the operational and functional life cycle of an IT application.	The SBE and LBEs have established policies and procedures for the AccuVote-TS voting system. However, these policies and procedures are neither complete, nor integrated. In addition, the information is dispersed between numerous documents at the SBE, LBE, and vendor levels.
Least privilege: The principle of least privilege is important to system integrity and requires that a user be given no more privilege than necessary to perform a job. Ensuring least privilege requires identifying what the user's job is, determining the minimum set of privileges required to perform that job, and restricting the user to a domain with those privileges and nothing more.	Only the minimum level of access to the AccuVote-TS system is granted to users. However, as noted in the Technical Controls section, generic user IDs are used for system level accounts which may circumvent the least privilege controls.
Security and technical training: Training provides users, either administrative or operational, with an understanding of the proper and legal use of the system. Security training is recommended for newly hired employees (initial training) before being permitted to access an IT system. Security training for current employees is recommended at least annually, but should be an on-going effort with a daily impact (security reminder posters, security warning banners, system broadcast messages, etc.).	The training materials for the AccuVote-TS voting system do not include an information security component.

Management Controls	
Principle	**AccuVote-TS Implementation**
Risk Assessment: Risk assessments provide SBE with an understanding of the threats and vulnerabilities to the system. Risk assessments should consider data sensitivity and the need for integrity and the range of risks to which an entity's systems and data may be subject, including those risks posed by authorized internal and external users, as well as unauthorized outsiders who may try to penetrate the systems. Such analysis should also draw on reviews of system and network configurations and observations and testing of existing security controls.	The SBE does not have a formal, implemented process for reviewing the impact of significant system modifications to the security controls for the AccuVote-TS voting system. Results from this risk assessment will serve as a baseline to determine the effectiveness of existing security controls and to provide recommendation for security deficiencies.
Incident response capability: This control covers guidance for the proper actions to be taken in the event an adverse action is taken against the system (e.g., hacker/cracker attempt, malicious code infection, user abuse of privileges).	The SBE Incident Management Plan provides a plan of action toward preparations and responses to incidents. However, there is no documentation that describes security controls to detect unauthorized transaction attempts by authorized and/or unauthorized users. Therefore, the application of security controls may be applied inconsistently, incorrectly, or incompletely.
Continuity of support: This control provides for the continued operation or recovery of operations following a natural or man-made disaster. Plans such as Contingency Plan (CP), Business Resumption (BR), Disaster Recovery (DR), and Continuity of Operations (COOP) are examples of the policies and procedures that provide for ensuring system availability.	The SBE Disaster Recovery and Incident Management Plan provides a plan of action for disaster recovery and contingency.
Assignment of responsibilities: Responsibilities for the protection of an IT system requires the delineation of duties consistent with the security principles of separation of duties and least privilege. Systems acquisition, management, operations, security, and audit make up individual functions that require oversight and compliance with federal and departmental regulation.	Registration and Election Laws of Maryland and COMAR define the authority, responsibility and accountability for assignment of responsibilities. However, a formal, documented System Security Plan has not been created, nor has documentation that identifies the process for maintaining appropriate access controls to the AccuVote-TS voting system.

5.3.2.Operational Controls Analysis

Operational controls focus on protection mechanisms that are primarily planned, implemented, and monitored by people.

Table 5-2: Operational Controls

Operational Controls	
Principle	**AccuVote-TS Implementation**
Maintenance of system integrity and availability: This control includes those measures taken to ensure the reliability of the system, including system and application development, system operational and security testing, and the appropriate application of operating system patches.	SBE has User Acceptance Testing Guidelines, Logic and Accuracy Testing Guidelines, and Disaster Recovery Guidelines. However, there is not a process to ensure that the implemented software version and firmware version of the AccuVote-TS voting system is the one certified by the ITA.
Application security plan: The Security Plan provides a framework for the protection of the information and information systems.	A Security Plan has not been created. However, there are various documents that contain security components at the SBE, LBE, and vendor levels.
Personnel clearance and background investigation: This control is intended to provide a means of assurance that all employees and contracted personnel meet a minimum level of trust and integrity.	The Election Judges Manual and The Election Administrator's Guide establish personnel security controls. However, background investigations are not performed for any individuals.
Periodic review of security controls: The establishment of a periodic evaluation of the security controls and mechanisms that protect system availability, integrity, and confidentiality; such as self-assessments, vulnerability scanning, and penetration testing.	This risk assessment is the first formal process for reviewing security controls. Results from this risk assessment will serve as a baseline to determine the effectiveness of existing security controls and to provide recommendation for security deficiencies.
Intrusion detection: Intrusion detection systems (IDS) are generally software-based products that provide real-time or near-real-time indications that an attack is occurring on the system. IDS can be either host-based (monitoring individual computers) or network-based (monitoring multiple computers on a network).	The components of the AccuVote-TS voting system are not connected to a network with the exception of the SBE GEMS server. IDS is not implemented on the SBE GEMS server.
Cryptography: Cryptography is important to the confidentiality of the information when stored, processed or transmitted. Encryption should meet federal standards under the Federal Information Processing Standards (FIPS) 140 series publications.	Cryptography is not employed for data stored on the PCMCIA cards, or transmitted data. DES is employed for memory only on the DRE voting terminal. When the DRE voting terminal is powered off its memory is cleared.

Operational Controls	
Principle	**AccuVote-TS Implementation**
Communications: Communications controls are those established to prevent or deter unauthorized users from accessing the system, such as the restrictions placed on accessible ports and IP addresses. Communications controls tie in strongly with access controls under the technical controls heading.	The security of the AccuVote-TS voting system is dependant upon the absence of any network connections. This requirement is met at the LBE level, but the SBE GEMS server is connected to the SBE intranet.
Environmental Controls: This control protects system equipment from operational damage due to extreme heat, extreme cold and contamination by airborne contaminates. This control also ensures the quality and availability of electrical power.	The GEMS servers and the DREs are maintained in environments suitable for operation and they are protected from power surges and brief power outages.
Facility Protection: Facility protection provides for the physical protection of the location housing the IT system equipment and personnel.	With the exception of the GEMS server located at SBE headquarters in Annapolis, the GEMS servers and the DREs are housed in appropriately secure locations both during and after elections. The SBE GEMS server is located in open space.
Media access, labeling, distribution, and disposal: These controls are for the protection of sensitive information both on electronic media (tape or disk) and hardcopy material. Physical protection against casual viewing, labeling with data sensitivity, distribution safeguards, and the proper disposition and disposal of electronic and hardcopy media are important to protect against social engineering and unauthorized access.	Each LBE Election Judge Manual has procedures approved by the SBE pertaining to the assembling, transport, and controls associated with the AccuVote-TS voting system components and outputs.
Configuration control and protection of workstations, laptops, servers, etc.: This control determines the strength of the protections afforded by the operating systems of the individual servers and workstations that connect to a network. Out-of-the-box operating systems generally require configuration changes in order to strengthen the system against known vulnerabilities.	The AccuVote-TS voting system is not connected to a network with the exception of the SBE GEMS server. However, several software vulnerabilities were noted in the source code for both the GEMS server and the DRE voting terminal. These findings are mitigated by process and procedures that keep these systems from being connected to an external network.

5.3.3.Technical Controls Analysis

Technical controls are generally system or electronically based and rely heavily on operational and management controls in addition to system based restrictions.

Table 5-3: Technical Controls

Technical Controls	
Principle	**AccuVote-TS Implementation**
System audit: System logs and access records form an audit trail of the system to provide a means of determining the "who, what, when, where, and how" associated with a system or security event. Audit logs provide the investigation record of a system and are critical files when an attack against the system has been detected or assumed.	The AccuVote-TS system logs occurrences of system events, however, these logs are not reviewed. In addition, GEMS Server audit logs are not configured to log any security events (i.e., extended logging) at the operating system level and the current log size is too small, therefore recorded events are overwritten. The operating system log is also not reviewed. Where there are logs, the logs are not backed up.
Identification and Authentication (I&A): I&A identifies an authorized user and validates that the user is authorized to use system resources. I&A is essential to system non-repudiation and is crucial to establishing logical access controls under a role-based paradigm for protecting system processes and information.	The AccuVote-TS system uses smartcard-based access to the DREs. However, for the GEMS servers, system account IDs with administrator privileges are shared and the passwords are not compliant with the State of Maryland Information Security Policy and Standards. In addition, the GEMS server does not lock the user accounts after a period of inactivity and it allows unlimited password guessing.
Logical access control: Logical access controls are those rights, privileges, and permissions granted to authorized users. While I&A establishes legitimacy to use the system, logical access controls determine what an authorized user is permitted to do while on the system. The user permissions to read, write, delete, and modify system files and objects are based on the principle of least privilege – granting only those rights and privileges needed by a user to accomplish their job function. Logical access control is the technical embodiment of the management control – the principle of least privilege.	Voters are restricted to proper access on the DREs. At the GEMS server access is restricted to administrator accounts. However, as noted above administrator IDs are shared and are not associated to a specific individual.
Maintenance of system integrity and availability: System maintenance during the life cycle of the system provides security mechanisms and controls to protect data integrity and availability. These controls account for additional devices and software, such as firewalls and IDS systems.	While many of the computer security controls are lacking, the risks have been mitigated because the AccuVote-TS voting system other than the SBE GEMS server is not connected to a network, and because the SBE has implemented a process to ensure that COMAR is adhered to for voting system integrity.

~~5.4.Step 5 – Likelihood Definition~~

~~Table 5-4, below, provides definitions of the likelihood ratings.~~

~~Table 5-4: Likelihood Definition~~

~~Likelihood Level~~	~~Likelihood Definition~~
~~HIGH~~	~~The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.~~
~~MEDIUM~~	~~The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.~~
~~LOW~~	~~The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the exercise of the vulnerability.~~

~~The "Likelihood" column of Table 5-8 presents the results of an analysis to determine qualitatively how likely it is that a particular vulnerability will be exploited by a particular threat source. A likelihood rating of High, Medium, or Low has been assigned to each threat/vulnerability pair. In the case of this risk assessment, all the evaluated threats are human, either intentional or unintentional. For this reason, the table does not list the threat source, since the threat source is identical throughout. The vulnerabilities and threat sources identified in Sections 5.1 and 5.2 have been input into the analysis. The analysis considers the effectiveness of the listed, existing security controls determined in Section 5.3, the nature of the vulnerability, and the capabilities and motivation of the threat source.~~

~~5.4.1.Likelihood Rating Rationale~~

~~The Likelihood rating rationale section of Table 5-8 provides the rating determined during the analysis stage and details the rationale for assigning the High, Medium, and Low ratings to the threat/vulnerability pairs, as shown in the Likelihood/Impact or Existing Controls column.~~

~~5.5.Step 6 – Impact Analysis~~

~~The impact analysis performed in this step measures the adverse impact to State of Maryland and the AccuVote-TS voting system, which could result from a successful exercise of a vulnerability by a threat source. Input to the impact analysis is the knowledge gained during system characterization (via both documentation review and interview of the system and data owners) regarding the AccuVote-TS voting system, the criticality of the data it transmits, and the sensitivity assigned to the system and its data.~~

~~The Impact (I) rating of High, Medium, or Low was assigned to each vulnerability were it to be successfully exploited by a threat. Table 5-5 contains the definition for each of the three levels.~~

Table 5-5: Magnitude of Impact Definition

Magnitude of Impact	Impact Definition
HIGH	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
MEDIUM	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede and organization's mission, reputation, or interest; or (3) may result in human injury.
LOW	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

5.5.1.Impact Rating Rationale

In addition to the qualitative rating, the Impact column in Table 5-8 provides the rationale in a summary statement addressing each rating according to the threat source.

5.6.Step 7 – Risk Determination

The threat likelihood ratings from Section 5.4 and the impact ratings from Section 5.5 are used in this step to develop a risk determination or rating. For each threat source/vulnerability pair, a qualitative risk rating was developed. The risk rating is dependent on three factors:

- The ability of planned or existing security controls to reduce or eliminate risk;
- The magnitude of the impact should a vulnerability be successfully exploited by a threat source; and
- The likelihood that a given threat source will attempt to exploit a particular vulnerability.

Section 3.7 of the NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, describes a methodology for determining risk levels. The NIST methodology also assigns the necessary actions for implementing corrective measures to each of three risk levels described in Table 5-6.

Table 5-6: Risk Rating/Implementation Correlation

Risk Rating	Action Implementation
HIGH	High-risk levels necessitate corrective actions and creation of an action plan that is put in place as quickly as possible.
MEDIUM	Medium-risk ratings warrant corrective actions and a plan to incorporate those actions within a reasonable period of time.
LOW	Low-risk levels present the application owner with a decision to accept the low risk or take corrective action.

The quantitative risk rating is computed based on the NIST SP 800-30 methodology and is shown in Table 5-7 below.

Table 5-7: Quantitative Risk Rating

Threat Likelihood	IMPACT		
	Low (10)	**Medium** (50)	**High** (100)
High (1.0)	Low 10 x 1.0 = 10	Medium 50 x 1.0 = 50	High 100 x 1.0 = 100
Medium (0.5)	Low 10 x 0.5 = 5	Medium 50 x 0.5 = 25	Medium 100 x 0.5 = 50
Low (0.1)	Low 10 x 0.1 = 1	Low 50 x 0.1 = 5	Low 100 x 0.1 = 10

Risk scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)

Table 5-8 shows the vulnerabilities discovered during the risk analysis. The first column gives the requirement number as either a managerial, operational, or technical control. The second column identifies the requirement against which the AccuVote-TS system was evaluated. The third column identifies whether or not the requirement was met, partially met, unmet or not applicable. The fourth column discusses the likelihood of a particular threat source exploiting the vulnerability, the impact of a successful exploit, and any existing controls that would mitigate the vulnerability. The fifth column in the table shows the overall risk rating. The sixth and final column discusses the mitigation for the risk.

The goal of the recommended control is to reduce the risk to the AccuVote-TS voting system and its data to an acceptable level. The following factors were considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g., system compatibility);

- Legislation and regulation;
- Organizational policy;
- Operational impact;
- Safety and reliability; and
- Cost.

5.7.Detailed Risk Assessment Results

Table 5-8 below depicts the detailed results of the Risk Assessment process. Each State of Maryland Baseline Security Requirement (BLSR) is compared to available information so that an assessment can be made as to the requirement having been met (M), partially met (P), or unmet (U). Where requirements are met, an analysis of the controls is included in the table. Where a requirement is unmet or only partially met, an analysis of the resulting vulnerability and risk is included, along with a suggested mitigation strategy. Some requirements are not applicable to the system as it exists today, but will serve to aid in future risk assessments should circumstances change.

Management controls address core or fundamental principles that are inherent in the protection of information systems to manage risk. Management requirements are considered met if the organization has a documented policy for meeting the requirement. Management controls do not judge the human or technical implementation of the policy, but do consider the policy's completeness and clarity.

Operational controls focus on protection mechanisms that are primarily planned, implemented, and monitored by people. Operational requirements are considered met if the organization has a human-based process in place for meeting the requirement. Operational controls judge the implementation and effectiveness of policies, but do not consider the presence of a documented policy.

Technical controls are generally system or electronically based and rely heavily on operational and management controls in addition to system-based restrictions. Technical requirements are considered met if the organization has a machine-based process in place for meeting the requirement. Technical controls judge the implementation and effectiveness of policies, but do not consider the presence of a documented policy.

Table 5-8: Requirement/Threat Source/Likelihood/Impact/Risk Rating/Mitigation

Management Controls

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
M-1	SBE will ensure that the voting election equipment will be accurate, reliable, and dependable.	M	Each LBE performs Logic and Accuracy testing before shipping the voting election equipment from the warehouses to ensure the equipment is accurate, reliable and dependable. Also all technicians performing the Logic and Accuracy testing must sign a confidentiality agreement.		
M-2	Systems security shall meet all Maryland System Security policy and standards.	U	If a system is not compliant with all Maryland System Security policy and standards, then the system may not provide confidentiality, integrity, or availability of the system data. In addition, it is a contractual requirement that the system security must meet Maryland System Security Policy and Standards in order to ensure the confidentiality, integrity, and availability of the system. The system does not meet all Maryland Information Security Policy and Standards as detailed in the analysis of the baseline security requirements. **Likelihood: HIGH** There are highly motivated and capable threat sources that may wish to alter election results. This analysis of the baseline security requirements has	HIGH	The State of Maryland should implement the recommendations as detailed in the following mitigation strategies associated with each vulnerability identified in Table 5.8. Ensure the electronic voting system meets all Maryland System Security policy and standards. Vendor issues that are identified as not meeting Maryland policy and standards should be documented and planned as a functional enhancement be delivered in the next software release or incremental release.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			identified many high-risk vulnerabilities with ineffective security controls. **Impact: HIGH** A successful attack may violate confidentiality, integrity, and/or availability of the system possibly delaying the SBE's mission and damaging its reputation or interests.		
M-3	SBE requires that all electronic voting equipment be certified by an Independent Test Authority (ITA) for evaluation against the Federal Election Commission (FEC) Voting System Standards prior to purchase and use.	**M**	The State of Maryland is required to use voting equipment hardware, software and firmware that are certified by an Independent Testing Authority as stated in the Code of Maryland Regulations. Wyle Labs and CIBER Inc. are the ITA that has certified the DRE hardware, software and firmware for the State of Maryland.		
M-4	SBE will confirm that the electronic voting equipment presented as certified is the same as the one qualified through the Standards.	**M**	The current version implemented throughout the state is certified by Wyle Labs and CIBER Inc. as meeting FEC voting system standards. Any future upgrades, patches etc. will need to go through the same testing process before being implemented.		
M-5	SBE will ensure the integrity of the voting system (i.e. processes, procedures, and technology).	**P**	If SBE does not ensure the integrity of the voting system, then the results of an election may not be accurate and the voter's rights may be violated. The State of Maryland has begun the process to ensure the integrity of the voting system as evidenced by this risk	**HIGH**	The State of Maryland should implement the recommendations as detailed in the following mitigation strategies associated with each vulnerability identified in Table 5.8. In addition, the State should implement an iterative process to ensure that the integrity of the voting system is maintained throughout the life cycle

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			assessment. In addition, SBE and LBE have established procedures designed to ensure the integrity of the voting system. However, these controls are neither complete, nor integrated. **Likelihood: HIGH** There are highly motivated and capable threat sources that may wish to alter election results. Since the controls are not complete nor integrated, the controls are not effective in ensuring the integrity of the voting system. **Impact: HIGH** A successful attack may violate confidentiality, integrity, and/or availability of the system possibly delaying the SBE's mission and damaging its reputation or interests.		process.
M-6	SBE will establish a baseline for future evaluations or tests of electronic voting system and processes, such as acceptance testing or state review after modifications have been made.	M	Results from this risk assessment will establish a baseline for future evaluations or tests of electronic voting system and processes. A risk assessment had not been conducted prior to this risk assessment.		
M-7	To ensure vote accuracy, SBE will ensure that all systems record the election contests, candidates, and issues exactly as defined by election officials.	M	The State of Maryland has implemented a process to ensure that COMAR 33.10.02.14 is met. This regulation states that at least 10 days before an election, the Election Management		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	as defined by election officials.		system and all voting units and accessible voting equipment shall be completely tested to ensure that they will accurately count the votes cast in all contests.		
M-8	To ensure vote accuracy, SBE will ensure that all systems record the appropriate options for casting and recording votes.	M	The State of Maryland has implemented a process to ensure that COMAR 33.10.02.14 is met. This regulation states that at least 10 days before an election, the Election Management system and all voting units and accessible voting equipment shall be completely tested to ensure that they will accurately count the votes cast in all contests.		
M-9	To ensure vote accuracy, SBE will ensure that all systems record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast.	M	The State of Maryland has implemented a process to ensure that COMAR 33.10.02.14 is met. This regulation states that at least 10 days before an election, the Election Management system and all voting units and accessible voting equipment shall be completely tested to ensure that they will accurately count the votes cast in all contests.		
M-10	SBE will ensure that ballots have been properly prepared and installed.	M	The State Board of Elections is the final authority to confirm ballot accuracy. Each of the LBEs verifies that the certified ballot is indeed accurate and includes all of the ballot styles in the election, ballot artwork and languages.		
M-11	SBE will document procedures that verify that voting machines	P	If SBE does not document procedures that verify that voting machines or vote	LOW	The State of Maryland should implement the recommendations as detailed in the

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~or vote recording and data processing equipment, precinct count equipment, and central count equipment are properly prepared for an election, and collect data that verifies equipment readiness.~~		~~recording and data processing equipment, precinct count equipment, and central count equipment are properly prepared for an election, and collect data that verifies equipment readiness, then the confidentiality, integrity, and availability of the voting system components may be compromised and security controls may be inconsistently applied.~~ ~~The SBE and LBEs have documented procedures and checklists in order to ensure that all electronic voting equipment is properly prepared for an election. However, these controls are neither integrated, nor located in a central repository.~~ ~~**Likelihood: LOW**~~ ~~The LBEs have established local procedures. These controls significantly impede the exploitation of the vulnerability.~~ ~~**Impact: MEDIUM**~~ ~~A successful attack may violate confidentiality, integrity, and/or availability of the system possibly delaying the organization's mission and damaging its reputation or interests.~~		~~following mitigation strategies associated with each vulnerability identified in Table 5.8. In addition, the State should consolidate and distribute standards and guidelines.~~
~~M-12~~	~~Local boards must follow processes developed and promulgated by SBE.~~	~~U~~	~~If the LBEs do not follow processes developed and promulgated by SBE, then security controls may be applied~~	~~LOW~~	~~In the future SBE should document procedures and distribute the procedures to all of the LBEs in order to achieve~~

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~promulgated by SBE.~~		~~inconsistently and the confidentiality, integrity, and availability of the system may be compromised.~~ ~~SBE has developed and documented some processes. However, this documentation is neither detailed nor complete. Currently policies are developed by the SBE, but each of the 24 LBEs develops and follows their own processes and procedures.~~ ~~**Likelihood: LOW**~~ ~~The LBE controls impede this vulnerability from being exercised. However, the lack of standards and metrics from SBE may result in error by election officials and technicians.~~ ~~**Impact: MEDIUM**~~ ~~If the vulnerability is exploited the validity and integrity of the election process may be compromised or may result in a violation of software licenses, theft, and unauthorized use.~~		~~standardization across the state. Standards and metrics allow performance, resource and cost justification decisions to be validated and accepted by management. By factoring standard procedures and metrics into the equation, performance and resource needs can be accurately assessed and justified in a more pro-active approach. Additionally, due to the variability and complexity inherent in most technology related incidents, standardization of processes, tools, methodologies and procedures is essential to ensure consistency and efficiency.~~
~~M-13~~	~~SBE employees and election officials must have professional integrity and be obligated to support the ethics programs at SBE.~~	~~M~~	~~Registration and Election Laws of Maryland article 2-101(d) and 2-103(c) state that the SBE and election officials must take the oath of office required by Article I, & 9 of the Maryland constitution.~~		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	Risk Rating	~~Mitigation Strategy~~
~~M-14~~	~~SBE should ensure that appropriate authority, responsibility and accountability are defined to accomplish the administration of the voting system, and that an appropriate organizational structure is established to effectively carry out program responsibilities.~~	~~M~~	~~Registration and Election Laws of Maryland and The Code of Maryland Regulations define the authority, responsibility and accountability to accomplish the administration of the voting system and establish the organizational structure.~~		
~~M-15~~	~~Key duties and responsibilities in authorizing, processing, recording, and reviewing voting transactions and processes should be separated among individuals.~~	~~M~~	~~Registration and Election Laws of Maryland, The Code of Maryland Regulations, Election Judge manuals and the Procedures for Official Canvass, Verification and Post-Election Audit describe and define and separates the key duties and responsibilities in authorizing, processing, recording, and reviewing voting transactions.~~		
~~M-16~~	~~SBE should exercise appropriate oversight to ensure individuals do not exceed or abuse their assigned authorities.~~	~~M~~	~~Registration and Election Laws of Maryland, The Code of Maryland Regulations, and Election Judge manuals provide appropriate oversight to ensure individuals do not exceed or abuse their assigned authorities.~~		
~~M-17~~	~~Access to resources and records should be limited to authorized individuals, and accountability for the custody and use of resources should be assigned and maintained.~~	~~M~~	~~Registration and Election Laws of Maryland, The Code of Maryland Regulations, and Election Judge manuals define who is authorized to access resources and records. Challengers and Watchers serve as an additional check for this requirement.~~		
~~M-18~~	~~Votes should be promptly recorded, properly classified~~	~~M~~	~~Votes are promptly recorded, classified and accounted for as described in the~~		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~recorded, properly classified and accounted for in order to prepare timely reporting, auditing and other reports.~~		~~and accounted for as described in the Registration and Election Laws of Maryland, COMAR, Election Judge manuals, and the Procedures for Official Canvass, Verification and Post-Election Audit.~~		
~~M-19~~	~~The documentation for transactions, management controls, and other significant events must be clear and readily available for examination.~~	~~P~~	~~If documentation for transactions, management controls, and other significant events is not clear and readily available for examination, then the security controls may be applied inconsistently or circumvented and the confidentiality, integrity, and availability of the system may be compromised.~~ ~~The State of Maryland has documentation that is clear, but not readily available.~~ ~~**Likelihood: LOW**~~ ~~The State of Maryland controls impede this vulnerability from being exercised. However, the lack of consolidated, available documentation may result in error by election officials and technicians.~~ ~~**Impact: LOW**~~ ~~If the vulnerability is exploited the validity and integrity of the election process may be compromised.~~	~~LOW~~	~~In the future SBE should consolidate procedures and distribute them to all of the LBEs in order to achieve standardization across the state.~~
~~M-20~~	~~SBE should promptly evaluate and determine proper actions in response to known deficiencies,~~	~~M~~	~~This risk assessment and the Risks, Issues, Systems Incidents and Changes (RISC) Plan enable SBE to evaluate and~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	reported audit and other findings, and related recommendations.		determine proper actions in response to known deficiencies and other findings and recommendations.		
M-21	Managers should continuously monitor and improve the effectiveness of security controls associated with the voting process.	M	SBE and LBEs continuously look for ways to improve the security controls of the voting process. The Change Control Process document enable managers to monitor and improve the effectiveness of security controls associated with the voting process. This risk assessment provides another tool to assist with this process.		
M-22	SBE and election officials should identify and report deficiencies, as this reflects positively on the agency's commitment to recognizing and addressing voting problems.	M	The Polling place evaluation process as stated in COMAR 33.07.03.04, Election Judge Manuals and the State of Maryland RISC database, ensure that deficiencies are identified and reported.		
M-23	SBE managers are responsible for taking timely and effective action to correct deficiencies, as appropriate.	M	The State of Maryland RISC Plan provides a framework for identifying and resolving issues and risks. It addresses all artifacts produced during the issue and risk management processes, including: □Risk and Issue descriptions □System Investigation Requests (SIR) □Change Requests (CR) and □Risk and Issue reports		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
M-24	The extent to which corrective actions are tracked by SBE should be commensurate with the severity of the deficiency.	M	The State of Maryland RISC plan provides the framework for identifying and resolving issues and risks. It addresses all artifacts produced during the issue and risk management processes, including: □Risk and Issue descriptions □System Investigation Requests (SIR) □Change Requests (CR) and □Risk and Issue reports		
M-25	Corrective action plans should be developed for all material weaknesses, and progress against plans should be periodically assessed and reported to SBE management.	M	The State of Maryland RISC plan provides the framework for identifying and resolving issues and risks. It addresses all artifacts produced during the issue and risk management processes, including: □Risk and Issue descriptions □System Investigation Requests (SIR) □Change Requests (CR) and □Risk and Issue reports		
M-26	The SBE security planning shall clearly delineate responsibilities and expected behavior of all individuals with access to the system.	M	Registration and Election Laws of Maryland, The Code of Maryland Regulations, Election Judge manuals and the Procedures for Official Canvass, Verification and Post-Election Audit delineate the responsibilities and		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			expected behavior of all individuals with access to the system.		
M-27	The SBE security planning shall include appropriate limits on interconnections to other systems.	M	Currently, the electronic voting system is not connected to any other system, with the exception of the SBE GEMS server. The SBE GEMS server is not used in the voting process. If there are plans to connect additional components of the voting system in the future, especially the DRE voting terminals, a thorough risk assessment will need to be conducted.		
M-28	The SBE security planning shall define service provision and restoration priorities.	M	The SBE Disaster Recovery and Incident Management Plan provides a plan of action with provision and restoration priorities.		
M-29	The SBE security planning shall be clear about the consequences of behavior not consistent with the rules.	M	Registration and Election Laws of Maryland, and The Code of Maryland Regulations describe the consequences of behavior not consistent with the rules.		
M-30	The SBE security planning shall ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system.	P	If the SBE security planning does not ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system, then the security controls may be applied inconsistently or circumvented and the confidentiality, integrity, and availability of the system may be compromised. The SBE has training for all of the election judges, poll workers and technicians. However, this training does	MEDIUM	Training should be established for security awareness and technical security training to ensure that election judges, poll workers and technicians are aware of the rules of behavior and their responsibilities in protecting the organization's mission. This training should include information about threats, vulnerabilities and risks to the voting system.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~not adequately address security issues.~~ ~~**Likelihood: MEDIUM**~~ ~~Without security awareness training the election judges, poll workers and technicians may not be aware of their security responsibilities.~~ ~~**Impact: HIGH**~~ ~~If the vulnerability is exploited the validity and integrity of the election process may be compromised.~~		
~~M-31~~	~~The SBE security planning shall contain rules of the system and indicate that periodic refresher training shall be required for continued access to the system.~~	~~P~~	~~If the SBE security planning does not contain rules of the system and indicate that periodic refresher training shall be required for continued access to the system, then the security controls may be applied inconsistently or circumvented and the confidentiality, integrity, and availability of the system may be compromised.~~ ~~The DESI contract with the SBE requires that designated election officials and staff receive training in the operation and management of the AccuVote-Touch Screen (AVTS), AccuVote-Optical Scan (AVOS) units, and Global Election Management System (GEMS) software. Many of the LBEs have developed their own training that is specific to their procedures and processes. However, this training does not adequately address~~	~~**MEDIUM**~~	~~Training should be established for security awareness and technical security training to ensure that election judges, poll workers and technicians are aware of the rules of behavior and their responsibilities in protecting the organization's mission. This training should include information about threats, vulnerabilities and risks to the voting system.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			security issues. **Likelihood: MEDIUM** Without security awareness training the election judges, poll workers and technicians may not be aware of their security responsibilities. **Impact: HIGH** If the vulnerability is exploited the validity and integrity of the election process may be compromised.		
M-32	The SBE's security planning for personnel controls shall require screening of individuals who are authorized to bypass significant technical and operational security controls of the system commensurate with the risk and magnitude of harm they could cause.	P	If the SBE's security planning for personnel controls does not require screening of individuals who are authorized to bypass significant technical and operational security controls of the system commensurate with the risk and magnitude of harm they could cause, then the security controls may be circumvented and the confidentiality, integrity, and availability of the system may be compromised. Personnel who are authorized to bypass technical and operational security controls do not currently go through a vetting process before being place into a position of trust. **Likelihood: LOW** SBE and LBE have implemented	**LOW**	Background investigations should be performed on senior election officials who have access to critical systems.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~controls to mitigate this risk including:~~ ~~□Two-person rule~~ ~~□Separation of duties~~ ~~□Least privilege~~ ~~□Confidentiality agreements~~ ~~**Impact: HIGH**~~ ~~Although the likelihood of an incident occurring at SBE is low, it could have significant impact on SBE's mission if exploited.~~		
~~M-33~~	~~The SBE's security planning for personnel controls screening shall occur prior to an individual being authorized to bypass controls and periodically thereafter.~~	~~**P**~~	~~If the SBE's security planning for personnel controls screening does not occur prior to an individual being authorized to bypass controls and periodically thereafter, then an individual may be granted inappropriate access and the confidentiality, integrity, and availability of the system may be compromised.~~ ~~Personnel who are authorized to bypass technical and operational security controls do not currently go through a vetting process before being place into a position of trust.~~ ~~**Likelihood: LOW**~~ ~~SBE and LBE have implemented~~	~~**LOW**~~	~~Background investigations should be performed on senior election officials who have access to critical systems before their initial access to systems is granted and periodically thereafter.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			~~controls to mitigate this risk including:~~ ~~□Two person rule~~ ~~□Separation of duties~~ ~~□Least privilege~~ ~~□Confidentiality agreements~~ ~~**Impact: HIGH**~~ ~~Although the likelihood of an incident occurring at SBE is low, it could have significant impact on SBE's mission if exploited.~~		
~~M-34~~	~~The SBE security planning shall ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats.~~	~~**M**~~	~~The SBE Disaster Recovery and Incident Management Plan provides a plan of action toward preparations and responses necessary to accomplish the following recovery goals after a disaster/incident occurs:~~ ~~□Determine, in a timely manner, whether the event is of sufficient magnitude and duration to cause unacceptable loss to SBE or LBE business operations~~ ~~□Ensure that appropriate advance measures have been taken to provide for the recovery of business operations in an acceptable period of time~~ ~~□Restore the affected resources or~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			provide a replacement for them within an acceptable period of time □Ensure appropriate internal and external communication is accomplished □Safeguard the public's confidence in elections.		
M-35	The SBE security planning Incident Response capability should assist SBE in pursuing appropriate legal action.	M	The SBE Disaster Recovery and Incident Management Plan along with the Registration and Election Laws of Maryland and The Code of Maryland Regulations assist the SBE in pursuing appropriate legal action.		
M-36	The SBE's security planning for continuity of support shall establish and periodically test the incident response capability to continue providing service within a system based upon the needs and priorities of the participants of the system.	M	The SBE Disaster Recovery and Incident Management Plan specifies review and update on an annual basis. The Incident Management Team Lead assembles the Incident Management Team every year to verify that the procedures are current.		
M-37	The SBE security planning shall ensure that cost-effective security products and techniques are appropriately used within the system.	U	If the SBE security planning does not ensure that cost-effective security products and techniques are appropriately used within the system, then funds may be spent for security controls that are not commensurate with the risk, funds may be depleted and not available for cost effective security controls, and the confidentiality, integrity, and availability of the system may be	MEDIUM	SBE should implement a process for ensuring that cost-effective security products and techniques are appropriately used in the system throughout the system lifecycle.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			compromised. SBE has not ensured that cost-effective security products and techniques are implemented. **Likelihood: MEDIUM** Without appropriately implemented, cost-effective security products and techniques, the system may not be adequately secured. **Impact: HIGH** If vulnerabilities are not exposed or fixed properly, the validity and integrity of the election process may be compromised.		
M-38	The SBE security planning shall require written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems.	P	If SBE security planning does not require written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems, then unplanned risks may be introduced to the system, the existing security controls may be circumvented and the confidentiality, integrity, and availability of the system may be compromised. Although the electronic voting system components other than the SBE GEMS server do not currently have any connections with other systems, SBE should have a process for requiring management approval prior for system interconnections.	LOW	Develop a process that requires management approval prior to system interconnections. This process should address the following: □Delineation of interconnection boundaries; □Responsibilities of interconnected agencies within established boundaries; □Roles, Responsibilities, and Points of contact for management officials in both organizations; □System Information protection;

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~interconnections.~~ ~~**Likelihood: LOW**~~ ~~There are currently no connections with other systems with the exception of the SBE GEMS server. Formal interconnection agreements provide both parties with minimum security requirements to limit system exposure against possible threats.~~ ~~**Impact: LOW**~~ ~~There are currently no connections with other systems other than the SBE GEMS server.~~		~~□Certification and Accreditation requirements;~~ ~~□Provisions for data sharing;~~ ~~□Emergency provision/notification procedures (especially for security incidents, disaster, termination or deployment of specific security controls, etc.);~~ ~~□Regular audits and security reviews, including provisions for penetration testing;~~ ~~□Minimum Availability and Service Level expectations;~~ ~~□Penalties and non-compliance.~~
~~M-39~~	~~Where system interconnection is authorized, controls shall be established and documented in SBE security planning that are consistent with the rules of the system and in accordance with DBM Standards.~~	~~**N/A**~~	~~The system does not have any authorized interconnections.~~		
~~M-40~~	~~SBE will review the security controls in each system when significant modifications are made to the system, or at least every three years, if no significant modifications are made.~~	~~**U**~~	~~If SBE does not review the security controls in each system when significant modifications are made to the system, or at least every three years, then unplanned risks may be introduced to the system, the existing security controls may be circumvented and the confidentiality, integrity, and availability~~	~~**HIGH**~~	~~System modifications should be reviewed through a formal implemented process to ensure that the changes do not negate any security controls that are currently in place.~~ ~~Results from this risk assessment will serve as a baseline to determine the~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			of the system may be compromised. SBE does not require a review of security controls when significant modifications are made. **Likelihood: HIGH** Since there is not a formal implemented process to review security controls, SBE cannot ensure that the controls are effective. **Impact: HIGH** Since SBE cannot ensure that the controls are effectivethe impact if this vulnerability were exploited, could be significant.		effectiveness of existing security controls and provide recommendations. Continue the risk assessment process at least every three years or whenever major changes occur throughout all phases of the system's life cycle.
M-41	SBE should also employ network security, including encryption for data in transit and protection for data at rest.	U	If SBE does not employ network security, including encryption for data in transit and protection for data at rest, then the confidentiality, integrity, and availability of the data may be compromised. SBE does not employ cryptography for data in transit. Cryptography would greatly reduce the chance of data being viewed by unauthorized sources if it were intercepted during transmission. **Likelihood: HIGH** Although the data is transmitted over a private point-to-point network, no cryptography is used to ensure the	**HIGH**	Implement cryptographic protocols for the data while it is transit such as hardware link-layer encryption (encrypting modems using 3DES or better encryption) or application-layer encryption (Secure Sockets Layer [SSL], Transport Layer Security [TLS], etc.).

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			integrity and confidentiality of the data being passed. Impact: HIGH A malicious user could intercept the data and read, modify or copy it during transmission.		
M-42	SBE security planning should concentrate the coordination of incident handling into one effort, thereby eliminating duplication of effort.	M	The SBE Disaster Recovery and Incident Management Plan does concentrate the coordination of incident handling efforts and describes the recommended recovery organizations of the SBE and the LBE. It identifies the roles and responsibilities of each team from the point of initial damage assessment until the actual execution of recovery activities.		
M-43	The SBE security planning incident handling requires not only the capability to react to incidents, but the resources to alert and disseminate the information to the appropriate personnel.	M	The SBE Disaster Recovery and Incident Management Plan outlines communication procedures that ensure the appropriate management and recovery team personnel have accurate and timely information.		
M-44	The designated Computer Security Program Manager (and support staff) should direct the organization's day-to-day management of its computer security program.	U	If the designated Computer Security Program Manager and support staff do not direct the organization's day-to-day management of the computer security program, then the security controls may be applied inconsistently or circumvented and the confidentiality, integrity, and availability of the system may be	LOW	Formally designate a Computer Security Program Manager to ensure that security issues are addressed and adhere to Maryland Security Policy and Standards.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~compromised.~~ ~~The SBE CIO directs the day-to-day IT operations of the organization, but there is no designated Computer Security Program Manager.~~ ~~**Likelihood: LOW**~~ ~~The security function is being performed by multiple individuals; therefore there is a relatively low likelihood of an attacker exploiting this vulnerability.~~ ~~**Impact: HIGH**~~ ~~The lack of a dedicated individual with accountability for the computer security program may result in security concerns not being addressed.~~		
~~M-45~~	~~Security plans should reflect input from various individuals with responsibilities concerning the system, including functional "end users," Information Owners, the System Administrator, and the Computer Security Program Manager.~~	~~M~~	~~The Polling place evaluation process, Election Judge Manuals and the SBE RISC Plan reflect input from various individuals regarding the system.~~		
~~M-46~~	~~SBE should have a policy on the security planning process.~~	~~M~~	~~DBM Security Policy and Standards covers the security planning process.~~		
~~M-47~~	~~Procedures should be in place outlining who reviews the System Security plans and~~	~~M~~	~~The SBE Disaster Recovery and Incident Management Plan describes a collaborative approach to project risk~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	follows up on planned controls.		management with state and county team members.		
M-48	Organizational policy should define who will provide the independent advice to the system security planning.	M	The State of Maryland has organizational policy for providing independent advice to the system security planning.		
M-49	Individuals providing advice to the system security planning should have adequate knowledge or experience to ensure the plan contains appropriate information and meets organizational security policy and standards.	M	The State of Maryland has contracted with individuals that have knowledge and experience to ensure the plan contains appropriate information and meets organizational security policy and standards.		
M-50	All system security plans, at a minimum, should be marked, handled, and controlled to the level of sensitivity determined by SBE policy.	M	DBM Security Policy and Standards requires security plans to be marked, handled, and controlled to the level of sensitivity commensurate with the risk.		
M-51	All System security plans should be dated for ease of tracking modifications and approvals.	M	All State of Maryland policies, plans and procedures are dated.		
M-52	The security plan should indicate the system's operational status (operational, under development, and /or undergoing a major modification), and if more than one status is selected, it should list which part of the system is	N/A	SBE does not have a security plan in place for this system. This resultant risk is addressed in requirement M-114.		

Number	~~Baseline Security Requirements~~	M/P/U /NA	~~Likelihood/Impact or Existing Controls~~	Risk Rating	Mitigation Strategy
	~~covered under each status.~~				
~~M-53~~	~~The system security planning should present a brief description of the function or purpose of the system and the information processed.~~	~~M~~	~~Vendor supplied documentation as well as COMAR provides descriptions and function of the system.~~		
~~M-54~~	~~The system security planning should list all applications supported by the general support system.~~	~~M~~	~~Vendor supplied documentation as well as COMAR provides listings of applications for the system.~~		
~~M-55~~	~~The system security planning should describe the processing flow of the application from system input to system output.~~	~~M~~	~~SBE has process workflows for the electronic voting system detailing system input and output.~~		
~~M-56~~	~~The system security planning should list user organizations (internal & external) and type of data and processing provided.~~	~~M~~	~~Each LBE has detailed organizational lists, type of data and processing for all of the voting precincts located within their jurisdiction.~~		
~~M-57~~	~~The system security planning should provide a general description of the technical system, and include any environmental or technical factors that raise special security concerns.~~	~~M~~	~~Vendor supplied documentation as well as the COMAR provides general technical descriptions and environmental factors of the system.~~		
~~M-58~~	~~The system security planning should describe the primary computing platform(s) used and a description of the principal system components, including hardware, software, and~~	~~M~~	~~Vendor manuals describe the primary computer platforms and the principal system components.~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	communications resources.				
M-59	The system security planning should include any security software protecting the system and information.	N/A	The system has no additional security software other than that provided by the native OS and the GEMS application. These security controls are addressed in the Technical Security Requirements.		
M-60	A description of the rules for interconnecting systems and for protecting shared data must be included with the system security planning.	N/A	The voting system does not currently have any connections with other systems, with the exception of the SBE GEMS server. The risks associated with the SBE GEMS server interconnections are described in the Operational and Technical Security Requirements.		
M-61	The system security planning should list any laws or regulations that establish specific requirements for confidentiality, integrity, or availability of data/information in the system.	M	The DBM IT Security Policy and Standards and COMAR provide specific requirements for confidentiality, integrity, or availability of data/information in the system.		
M-62	The system security planning should describe, in general terms, the information handled by the system and the need for protective measures; relate the information handled to each of the three basic protection requirements (confidentiality, integrity, and availability); and for each of the three categories, indicate if the requirement is: High, Medium, or Low.	M	Results from this risk assessment will determine the effectiveness of existing security controls and provide recommendations for mitigating the identified risks. Note: This risk assessment is the first performed on the Accuvote-TS voting system.		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
M-63	The system security planning should include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system.	M	Results from this risk assessment will determine the effectiveness of existing security controls and provide recommendations for mitigating the identified risks. Note: This risk assessment is the first performed on the Accuvote-TS voting system.		
M-64	The system security planning should describe the risk assessment methodology used to identify the threats and vulnerabilities of the system, and include the date the review was conducted.	M	This risk assessment describes the methodology used to identify the threats and vulnerabilities of the system and includes the date this review was conducted. Note: This risk assessment is the first performed on the Accuvote-TS voting system.		
M-65	If there is no system risk assessment, the system security planning should include a milestone date (month and year) for completion of the assessment.	M	This risk assessment satisfies this requirement. Note: This risk assessment is the first performed on the Accuvote-TS voting system.		
M-66	The system security planning should list any independent security reviews conducted on behalf of the state on the system in the last three years.	M	This risk assessment satisfies this requirement. Note: This risk assessment is the first performed on the Accuvote-TS voting system.		
M-67	The system security planning should include information	M	If the system security planning does not include information about the type of		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	about the type of security evaluation performed, who performed the review, the purpose of the review, the findings, and the actions taken as a result.		security evaluation performed, who performed the review, the purpose of the review, the findings, and the actions taken as a result, then the results of the assessment may be misinterpreted or not relevant, and the confidentiality, integrity, and availability of the system may be compromised. Results from this risk assessment determine the effectiveness of existing security controls and provide recommendations for mitigating the identified risks. Note: This risk assessment is the first performed on the Accuvote-TS voting system.		
M-68	If the system or part of the system is in the initiation phase, the system security planning should reference the sensitivity of information handled.	N/A	The system is not in the initiation phase.		
M-69	The system security plan should, during the first part of the development/ acquisition phase, include security requirements, which are developed at the same time system planners define the requirements of the system.	N/A	The system is not in the development/ acquisition phase.		
M-70	If the system or part of the system is in the development/ acquisition phase, the system	N/A	This system is not in the development/ acquisition phase.		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	security planning should include a general description of any specifications that were used and whether they are being maintained.				
M-71	If the system or parts of the system are in the operation/ maintenance phase, the system security planning should document the security activities conducted or planned for in that part of the system.	M	The system is in the operational phase and this Risk Assessment along with the RISC database documents the security activities conducted and planned.		
M-72	The system security planning should provide the date of authorization, name, and title of management official authorizing processing in the system.	M	The SBE has authorized use of this system.		
M-73	If the system is not authorized, the system security planning should provide the name and title of manager requesting approval to operate and date of request.	N/A	The SBE has authorized use of this system.		
M-74	The system security planning should include detailed information on whether all positions have been reviewed for sensitivity level, and if not, statement on the planned date for completion of position sensitivity analysis.	U	If the system security planning does not include detailed information on whether all positions have been reviewed for sensitivity level, and if not, statement on the planned date for completion of position sensitivity analysis, then an individual may be granted inappropriate access and the confidentiality, integrity, and availability of the system may be	LOW	SBE and LBE should implement a formal process for reviewing position descriptions for sensitivity levels on a periodic basis.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~compromised.~~ ~~SBE and LBE do not have a process for reviewing position descriptions for sensitivity levels.~~ ~~SBE and LBE have implemented controls to mitigate this risk including:~~ ~~□Two person rule~~ ~~□Separation of duties~~ ~~□Least privilege~~ ~~□Confidentiality agreements~~ ~~**Likelihood: LOW**~~ ~~While the likelihood of occurrence at the LBE is more likely, the LBE has implemented controls to mitigate this vulnerability. The likelihood at SBE is low, but minimal controls have been implemented.~~ ~~**Impact: HIGH**~~ ~~Although the likelihood of an incident occurring at SBE is low due to this vulnerability, it's exploitation could have significant impact on SBE's mission~~		
~~M-75~~	~~The system security planning should include a statement as to whether individuals have received background~~	~~**N/A**~~	~~No background screenings are conducted. The necessity for background screening is addressed in requirement M-32.~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	screenings appropriate for the position to which they are assigned, and if not, the date by which such screening will be completed should be included.		requirement M-32.		
M-76	The system security planning should describe conditions under which individuals are permitted system access prior to completion of appropriate background screening and any compensating controls to mitigate associated risk.	N/A	No background screenings are conducted. The necessity for background screening is addressed in requirement M-32.		
M-77	The system security planning should include detailed information on whether the type of user access is restricted to the minimum necessary to perform the job (i.e., least privilege).	M	Least Privilege is practiced throughout the SBE and LBEs by the checks and balances of the election process.		
M-78	The system security planning should include detailed information on the process for requesting, establishing, issuing, and closing user accounts.	U	If the system security planning does not include detailed information on the process for requesting, establishing, issuing, and closing user accounts, then an individual may be granted or continue to exercise inappropriate access and the confidentiality, integrity, and availability of the system may be compromised. There is currently not a process in place for establishing, issuing, and closing user accounts on the GEMS server.	MEDIUM	SBE should establish and follow a formal process for requesting, establishing, issuing and closing user accounts. Administrators should periodically delete disabled or dormant accounts after obtaining management approval. Implement a formal policy on dormant account deletion to reduce this risk.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~**Likelihood: MEDIUM**~~ ~~Unless accounts are closed promptly, users that no longer require access could continue to access the system. This is a common access means that terminated and disgruntled employees use to cause harm to their former employers. While the potential threat source may be highly motivated, other security controls such as physical security controls are in place.~~ ~~**Impact: HIGH**~~ ~~Having inactive user accounts or the use of default accounts increases the possibility of unauthorized viewing and/or exploitation of sensitive data or system settings.~~		
~~M-79~~	~~The system security planning should include detailed information on how critical functions are divided among different individuals (i.e., separation of duties).~~	~~**P**~~	~~If the system security planning does not include detailed information on how critical functions are divided among different individuals (i.e., separation of duties), then an individual may be granted inappropriate access and the confidentiality, integrity, and availability of the system may be compromised.~~ ~~Separation of Duties is practiced when possible. Lack of resources at the SBE and LBEs make total separation of duties impractical.~~ ~~**Likelihood: MEDIUM**~~	~~**MEDIUM**~~	~~Perform Separation of Duties of critical functions.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			~~There are effective deterrents for misusing system privileges.~~ ~~**Impact: MEDIUM**~~ ~~This vulnerability could impact SBE's mission if exploited.~~		
~~M-80~~	~~The system security planning should include detailed information on what mechanisms are in place for holding users responsible for their actions.~~	~~**M**~~	~~Registration and Election Laws of Maryland and COMAR hold users responsible for their actions.~~		
~~M-81~~	~~The system security planning should include detailed information on the kind of friendly or unfriendly termination procedures used.~~	~~**U**~~	~~If the system security planning does not include detailed information on the kind of friendly or unfriendly termination procedures used, then a terminated employee may have unauthorized access to the system which may result in the loss of confidentiality, integrity, and availability of the system.~~ ~~There are not documented procedures for handling the termination of an election official or technician with administrator access. Without an established process for promptly closing user accounts upon termination, unauthorized system access may occur.~~ ~~**Likelihood: MEDIUM**~~ ~~Unless accounts are closed promptly, users that no longer require access could~~	~~**MEDIUM**~~	~~Privilege revocation procedures should be developed to address the possibility of a disgruntled election official or system technician.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			~~continue to access the system. This is a common access means that terminated and disgruntled employees use to cause harm to their former employers. While the potential threat source may be highly motivated, other security controls such as physical security controls are in place.~~ ~~**Impact: HIGH**~~ ~~Disgruntled former employees could have unauthorized viewing and/or exploitation of sensitive data or system settings.~~		
~~M-82~~	~~System security planning should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting systems (such as electric power), backup media, and any other elements required for system's operation.~~	~~**M**~~	~~Vendor manuals and election judge manuals address all of the elements required for system operations.~~		
~~M-83~~	~~System security planning should describe physical protection controls, specifically physical protection for the system, the area where processing takes place, and physical access.~~	~~**M**~~	~~Vendor manuals, election judge manuals, and the SBE Implementation Plan describe physical protection controls at the polling places as well as the warehouses where equipment is stored.~~		
~~M-84~~	~~System security planning should address fire safety, failure of supporting utilities,~~	~~**M**~~	~~The SBE Disaster Recovery and Incident Management Plan addresses fire safety, failure of supporting utilities, structural~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	structural collapse, plumbing leaks, interception of data, mobile and portable systems.		collapse, plumbing leaks, interception of data, mobile and portable systems.		
M-85	System security planning should describe the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media.	M	The COMAR and the Implementation Plan describe the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media.		
M-86	System security planning should list controls used to monitor the installation of, and updates to, software.	M	The COMAR 33.09.05.12 and ITA certification satisfies this requirement.		
M-87	System security planning should describe the establishment of a user support help desk or group that can offer advice.	M	Vendor supplied support and LBE trained technicians provide help desk support.		
M-88	System security planning should describe procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information.	M	In their aggregation, the processes and procedures contained in the Election Judge manuals, Implementation Plan, Administrators Guide and Disaster Recovery and Incident Management Plan satisfy this requirement in totality.		
M-89	System security planning should describe procedures for ensuring that only authorized users pick up, receive, or deliver equipment, input and	M	The SBE AccuVote Touch Screen Voting System Phase II Implementation Plan describes procedures for ensuring that only authorized users pick up, receive, or deliver equipment, input and output		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~output information and media.~~		~~information and media.~~		
~~M-90~~	~~The system security planning should describe the use of audit trails for receipt of sensitive inputs/outputs.~~	~~M~~	~~The GEMS Server Administration guide describes the use of audit trails for receipt of sensitive election inputs/outputs.~~		
~~M-91~~	~~System security planning should describe procedures for restricting access to output products.~~	~~M~~	~~Access to output products, i.e., the election results, is restricted to individuals with a need to know as described in the Election Judge Manual, 2002 Election Results Transfer Memorandum, and Election Night Results Processing.~~		
~~M-92~~	~~System security planning should describe procedures and controls used for transporting Diebold equipment and election results.~~	~~M~~	~~The SBE AccuVote-Touch Screen Voting System Phase II Implementation Plan, Election Judge manuals, Election Administrator Guide describes procedures and controls used for transporting Diebold equipment and election results.~~		
~~M-93~~	~~System security planning should describe the use of internal/external labeling for sensitivity.~~	~~N/A~~	~~No labeling is used for sensitivity levels.~~		
~~M-94~~	~~The system security planning should describe the use of external labeling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates).~~	~~N/A~~	~~No labeling is used for sensitivity levels.~~		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
~~M-95~~	~~System security planning should describe the use of audit trails for inventory management.~~	~~M~~	~~The SBE AccuVote Touch Screen Voting System Phase II Implementation Plan, Election Judge manuals, Election Administrator Guide describes the use of audit trails for inventory management.~~		
~~M-96~~	~~System security planning should describe media storage vault or library physical, environmental protection controls/procedures.~~	~~M~~	~~The SBE AccuVote Touch Screen Voting System Phase II Implementation Plan, Election Judge manuals, Election Administrator Guide describes media storage vault or library physical, environmental protection controls/procedures.~~		
~~M-97~~	~~System security planning should describe procedures for sanitizing electronic media for reuse (e.g., overwriting or degaussing electronic media).~~	~~M~~	~~COMAR article 33.10.01.41 describes procedures for reuse (e.g., overwriting or degaussing electronic media).~~		
~~M-98~~	~~System security planning should describe procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse.~~	~~P~~	~~If system security planning does not describe procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse, then the media may be obtained by an unauthorized user.~~ ~~The COMAR article 33.10.01.41 describes procedures for controlled storage and handling of results media. The destruction of spoiled media is not addressed.~~ ~~**Likelihood: MEDIUM**~~	~~**LOW**~~	~~Develop and implement a policy for destroying spoiled media.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			An attacker may exploit this vulnerability by gaining access to spoiled media that is improperly discarded. **Impact: LOW** Once an election is concluded, the media does not contain sensitive information. Election results, once released, are public information. Spoiled media, such as PCMCIA cards that may be improperly discarded during an election could potentially be recovered using advanced techniques. However, the information that could potentially be recovered from an individual PCMCIA card would be of little value, as it would be limited to vote information from a single terminal.		
M-99	System security planning should describe procedures for shredding or other destructive measures for hardcopy media when no longer required.	U	If system security planning does not describe procedures for shredding or other destructive measures for hardcopy media when no longer required, then information may be inadvertently disclosed to unauthorized individuals resulting in the potential loss of confidentiality of the voting system. There are no procedures that address user actions for disposing of system documentation to prevent unauthorized viewing. **Likelihood: HIGH**	**MEDIUM**	Develop and implement a policy for destroying hardcopy media when no longer required.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~There are no controls to ensure that system documentation is destroyed when no longer needed, an attacker is can exploit this vulnerability by gaining access to improperly disposed of sensitive documentation.~~ ~~**Impact: MEDIUM**~~ ~~A successful attack may violate confidentiality, integrity, and/or availability of the system possibly delaying the SBE's mission and damaging its reputation or interests.~~		
~~M-100~~	~~System security planning should describe contingency plan procedures that would be followed to ensure the system continues to process all processes if a disaster should occur and provide a reference to the detailed plans.~~	~~M~~	~~The SBE Disaster Recovery and Incident Management Plan details the procedures for the SBE and LBE to recover from a disaster/incident.~~		
~~M-101~~	~~System security planning should address procedures in place to ensure that maintenance and repair activities are accomplished without adversely affecting the security of the system.~~	~~M~~	~~The legal agreement with Diebold includes provisions for compliance with the State of Maryland Information and Security Policy and Standards.~~		
~~M-102~~	~~System security planning should describe configuration management procedures for the system.~~	~~M~~	~~The SBE AccuVote Voting System Change Control Plan outlines the standard and systematic process that will be used for all Change Requests for the AccuVote-TS voting system project~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			AccuVote-TS voting system project.		
M-103	System security planning should describe policies for handling copyrighted software or shareware.	M	The State of Maryland Information and Security Policy and Standards contain policies for handling copyrighted software or shareware.		
M-104	System security planning should describe any controls that provide assurance to users that the information has not been altered and that the system functions as expected.	M	In their aggregation, the processes and procedures contained in the Election Judge manuals, Implementation Plan, Administrators Guide and Disaster Recovery and Incident Management Plan satisfy this requirement.		
M-105	System security planning should list the documentation maintained for the general support system.	M	SBE has a listing of documentation for the electronic voting system.		
M-106	System security planning requires a standardized log-on banner where appropriate be included in the system documentation.	M	The log on banner is detailed in the State of Maryland Information and Security Policy and Standards.		
M-107	System security planning should include information on security awareness and training.	U	If system security planning does not include information on security awareness and training then the security controls may be applied inconsistently or circumvented and the confidentiality, integrity, and availability of the system may be compromised. The training for the electronic voting system does not include an information security component. The increasing number of threats to IT systems has	HIGH	Implement a formal security awareness, training, and education program appropriate for each user's level of access.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			resulted in the need for security awareness, training, and education at all levels. Failure to conduct security awareness, training and education leaves election officials at all levels potentially unaware of the vulnerabilities and threats to their system. Without this awareness, the officials may not correctly or completely carry out vital security duties. **Likelihood: HIGH** Since the security of the AccuVote-TS system relies on non-technical controls performed by personnel, such as election judges, this awareness is vital to ensuring the security of the system. The lack of a security awareness training program provides an opportunity for a motivated attacker to exploit the system. **Impact: HIGH** The impact of the election officials potentially failing to carry out vital security duties could significantly impair the SBE mission.		
M-108	System security planning should describe incident handling procedures in place for the general support system.	M	The SBE Disaster Recovery and Incident Management Plan, The Risks, Issues, Systems Incidents, and Changes (RISC) Plan and Election Judge manuals describe incident handling procedures.		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
M-109	System security planning should describe how the general support system identifies access to the system, specifically, unique identification, correlate actions to users, maintenance of user IDs, and inactive user IDs.	U	If system security planning does not describe how the general support system identifies access to the system, specifically, unique identification, correlate actions to users, maintenance of user IDs, and inactive user Ids, then an individual may be granted inappropriate access and the confidentiality, integrity, and availability of the system may be compromised. There is no documentation that identifies the process for maintaining appropriate access controls for the system. Lack of proper documentation has resulted in the vendor default settings being left in place with the default user ID and password in the configurations. This information (i.e., passwords) is also documented in various manuals. **Likelihood: HIGH** Vendor default settings are in place with the default user ID and password in the configurations. This password information is also documented in various manuals, thus making this vulnerability easily exploitable. **Impact: HIGH** An unauthorized user that gains access to the system via the default and/or published user ID and password will be able to take any action that an authorized user could take. These actions include accessing sensitive information,	HIGH	Document procedures that describe how the general support system identifies access to the system, specifically, unique identification, correlate actions to users, maintenance of user IDs, and inactive user IDs. Ensure that the identification and authentication and auditing mechanisms employed comply with State of Maryland Security Policies and Standards.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			introducing malicious code, deleting or modifying data, and impeding the mission of the SBE.		
M-110	System security planning should describe the general support system's authentication control mechanisms.	M	In their aggregation, the processes and procedures contained in the Election Judge manuals, Implementation Plan, Administrators Guide and Disaster Recovery and Incident Management Plan satisfy this requirement.		
M-111	System security planning requires the minimum number of characters for a password to be between six and eight characters in a combination of alpha, numeric, or special characters.	U	If system security planning does not require the minimum number of characters for a password to be between six and eight characters in a combination of alpha, numeric, or special characters, then passwords may be guessed resulting in an individual being granted inappropriate access and the confidentiality, integrity, and availability of the system may be compromised. This requirement fails due to the use of vendor supplied default passwords, which do not meet the State of Maryland Information Security Policy and Standards. Therefore, passwords may be easily compromised. **Likelihood: MEDIUM** With physical access to the system and the assistance of a password dictionary or similar password cracking software, or by brute force, the threat source can figure out the password and authenticate to the system as a legitimate user. This	**MEDIUM**	The system should adhere to the State of Maryland Security Policy and Standards for password complexity.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			can be more damaging if the exploited user account has elevated privileges. Impact: HIGH Unauthorized logon use can result in a variety of consequences ranging from accessing, sensitive information and introducing malicious code, to the destruction, modification, and/or defacement of data, impeding the mission of the SBE and its image/trust among its customers, peers, and the general public.		
M-112	System security planning should discuss logical access controls in place to authorize or restrict the activities of users and system personnel within the general support system.	M	In their aggregation, the processes and procedures contained in the Election Judge manuals, Implementation Plan, Administrators Guide and Disaster Recovery and Incident Management Plan satisfy this requirement.		
M-113	System security planning should describe hardware and software features designed to permit only authorized access to or within the system, to restrict users to authorized transactions and functions, and/or to detect unauthorized access activities.	M	The vendor-supplied manuals describe hardware and software features designed to permit only authorized access and transactions, particularly through the use of the voter access cards.		
M-114	There should be a System Security Plan, which should: (1) Describe formal policies that define the authority that will be	U	If there is a not a System Security Plan, that: 1) Describes formal policies that define the authority that will be granted to each	HIGH	SBE should develop and document a System Security Plan. The System Security Plan should: (1) Describe formal policies that define

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	granted to each user or class of users; (2) Indicate if these policies follow the concept of least privilege which requires identifying the user's job functions, determining the minimum set of privileges required to perform that function, and restricting the user to a domain with those privileges and nothing more; and, (3) Include in the description the procedures for granting new users access and the procedures for when the role or job function changes.		user or class of users; 2) Indicates if these policies follow the concept of least privilege which requires identifying the user's job functions, determining the minimum set of privileges required to perform that function, and restricting the user to a domain with those privileges and nothing more; and, (3) Includes in the description the procedures for granting new users access and the procedures for when the role or job function changes, then the security controls may be applied inconsistently or circumvented and the confidentiality, integrity, and availability of the system may be compromised. There is no System Security Plan for the electronic voting system. The purpose of the system security plan is to provide an overview of the security requirements of the system and describe controls in place or planned responsibilities and expected behavior of all individuals who access the system. **Likelihood: HIGH** The System Security Plan provides the mechanism for structured planning of adequate, cost-effective security controls for the system. Without the System Security Plan control, a threat source		the authority that will be granted to each user or class of users; (2) Indicate if these policies follow the concept of least privilege, which requires identifying the user's job functions, determining the minimum set of privileges required to perform that function, and restricting the user to a domain with those privileges and nothing more; and, (3) Include in the description the procedures for granting new users access and the procedures for when the role or job function changes.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			may exploit vulnerabilities that are inherent to the system and that do not have adequate security controls in place. **Impact: HIGH** This vulnerability can expose the SBE's data to destruction, alteration, disclosure, and unavailability of critical system resources, impeding or delaying its mission, and damaging its reputation or interest.		
M-115	The System security planning should describe the system's capability to establish an Access Control List or register of the users, and the types of access they are permitted.	**M**	The SBE and LBEs have a manual register of users and technicians throughout the precincts and each of their respective areas of coverage. The SBE and LBE procedures specify the access each group of users is allowed to possess.		
M-116	System security planning should indicate whether a manual Access Control List is maintained.	**M**	The SBE and LBEs have a manual register of users and technicians throughout the precincts and each of their respective areas of coverage.		
M-117	System security planning should indicate if the security software allows application owners to restrict the access rights of other application users, the general support system administrator, or operators to the application programs, data, or files.	**M**	In their aggregation, the processes and procedures contained in the Election Judge manuals, Implementation Plan, Administrators Guide and vendor manuals satisfy this requirement.		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
M-118	System security planning should describe how application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties.	M	In their aggregation, the processes and procedures contained in the Election Judge manuals, Implementation Plan, Administrators Guide and vendor manuals satisfy this requirement by ensuring the principle of least privilege.		
M-119	The System security planning should indicate how often Access Control Lists are reviewed to identify and remove users who have left the organization or whose duties no longer require access to the application.	U	If the System security planning does not indicate how often Access Control Lists are reviewed to identify and remove users who have left the organization or whose duties no longer require access to the application, then an individual may retain inappropriate access and the confidentiality, integrity, and availability of the system may be compromised. System security planning documents do not indicate that Access Control Lists are reviewed regularly to identify and remove users who no longer require access. **Likelihood: MEDIUM** This vulnerability could be exploited if a user changes job functions or leaves the organization and is not removed from the system. **Impact: MEDIUM** Users that no longer require access to the system may view information that they are unauthorized to view or may	**MEDIUM**	SBE should generate, maintain, and secure a list of approved users and their accesses. Maintaining a current list of approved users and their accesses will reduce the likelihood of leaving privileges unchanged when users change job functions or leave the organization.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			change system settings inappropriately..		
M-120	System security planning should describe policy or logical access controls that regulate how users may delegate access permissions or make copies of files or information accessible to other users, and document any evaluation made to justify/support use of "discretionary access control.	P	If system security planning does not describe policy or logical access controls that regulate how users may delegate access permissions or make copies of files or information accessible to other users, and document any evaluation made to justify/support use of "discretionary access control, then unauthorized individuals may gain access to the information and the confidentiality, integrity, and availability of the system may be compromised. DAC or MAC provide for granular security. Vendor guides describe how both the server and the voting terminals practice discretionary and mandatory access controls over the data. However, copying of files or information is not covered. Lack of controls over data duplication may result in a user viewing data that was not explicitly authorized for the user to view. **Likelihood: MEDIUM** Without proper controls specifying the rules for the copying of information, an authorized user may make copies for unauthorized individuals.	LOW	SBE should develop and document a System Security Plan that includes controls specifying who is authorized to make copies of files or information accessible to other users.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			Impact: LOW While the copying of information may result in damage to SBE or LBE's reputation, it would not significantly impact the SBE and LBE mission.		
M-121	System security planning should describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users.	U	If system security planning does not describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users, then unauthorized attempts may go undetected resulting in the failure to identify new and emerging threat sources which may eventually lead to the compromise of the system confidentiality, integrity, and/or availability. There is no documentation that describes controls to detect unauthorized transaction attempts by authorized and/or unauthorized users. Likelihood: HIGH Threat sources are more likely to exploit a system if evidence against his/her actions cannot be gathered or obtained. Impact: HIGH The absence of this security control may lead to unauthorized, undetected, or unknown system access orchanges to system settings, resulting in significant impairment of the SBE mission.	HIGH	Document and implement security controls to detect unauthorized transaction attempts by authorized and/or unauthorized users.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
~~M-122~~	~~Logical access controls in the system security planning should indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.~~	~~M~~	~~The State of Maryland Information and Security Policy and Standards indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.~~		
~~M-123~~	~~System security planning should describe any restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends, and discuss in-place restrictions.~~	~~N/A~~	~~The systems are only in use during scheduled elections and in authorized election preparation activities.~~		
~~M-124~~	~~System security planning should discuss cryptographic methodology and key management procedures, if encryption is used.~~	~~N/A~~	~~If system security planning does not discuss cryptographic methodology and key management procedures, if encryption is used, then weak or poor cryptography may be implemented resulting in the potential disclosure or modification of sensitive information by unauthorized users.~~ ~~Encryption is not used for data stored on the PCMCIA cards or the transmissions from the DRE to the GEMS server. The data in DRE memory is encrypted using DES, but the memory is cleared when~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			the machine is powered off.		
M-125	The system security planning should discuss additional hardware or technical controls installed and implemented to provide protection against unauthorized system penetration and other known Internet threats and vulnerabilities, if general support system is connected to the Internet or other wide area network.	N/A	If the system security planning does not discuss additional hardware or technical controls installed and implemented to provide protection against unauthorized system penetration and other known Internet threats and vulnerabilities, when the support system is connected to the Internet or other wide area network, then unplanned risks may be introduced to the system and the existing security controls may be circumvented and the confidentiality, integrity, and availability of the system may be compromised. There are no additional hardware or technical controls installed or implemented on the SBE GEMS server for discussion.		
M-126	System security planning should describe any type of secure gateway or firewall in use, including its configuration.	N/A	A firewall is not in use.		
M-127	System security planning should provide information regarding any port protection devices used to require specific access authorization to the communication ports, including the configuration of the port protection devices and if additional passwords or tokens are required.	N/A	If system security planning does not provide information regarding any port protection devices used to require specific access authorization to the communication ports, including the configuration of the port protection devices and if additional passwords or tokens are required, then the security controls may be applied inconsistently or circumvented and the confidentiality, integrity, and availability of the system		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			may be compromised. There are not any port protection devices in use.		
M-128	System security planning should identify whether internal security labels are used to control access to specific information types or files, and if such labels specify protective measures or indicate additional handling instructions.	N/A	There are no security labels used to control access in the electronic voting process.		
M-129	System security planning should indicate if host-based authentication is used.	N/A	Host based authentication is not used.		
M-130	System security planning should describe the rationale for electing to use or not use warning banners and provide an example of the banners used.	M	The log on banner is detailed in the State of Maryland Information and Security Policy and Standards.		
M-131	The security planning should describe audit trail mechanisms in place.	M	The Election Judge manuals and the Election Administrator Guide describe manual audit trail mechanisms through the use of signed affidavits and checklists. The GEMS server administrator guide describes audit trail mechanisms on the server side.		
M-132	System security planning should address if the audit trails provide accountability by providing a trace of user	M	The Election Judge manuals and the Election Administrator Guide provide accountability through the use of signed affidavits and checklists. The GEMS		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	actions.		server administrator guide describes audit trail mechanisms on the server side.		
M-133	System security planning should address if the audit trails support after-the-fact investigations of how, when, and why normal operations ceased.	U	If system security planning does not address if the audit trails support after-the-fact investigations of how, when, and why normal operations ceased, then audit trails may be incomplete and the confidentiality, integrity, and availability of the system may be compromised. There is no documentation requiring the review of audit trails. Without regular event log review, it is very difficult to identify when any improper use of the system has occurred. **Likelihood: HIGH** Without regular audit log reviews, intrusion or intrusion attempts could go undetected. **Impact: HIGH** Both intentional and unintentional human threats can cause damage to the system and without audit log review, inappropriate system activity may not be detected. Exercise of this vulnerability could result in significant impairment to the SBE mission.	**HIGH**	A formal and documented process requiring the review of audit logs should be implemented.
M-134	System security planning should address if the audit trails are designed and implemented	U	If system security planning does not address if the audit trails are designed and implemented to record appropriate	**HIGH**	Implement a formal and documented process describing the proper configuration of audit trails.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	to record appropriate information that can assist in intrusion detection.		information that can assist in intrusion detection, then audit trails may be incomplete and the confidentiality, integrity, and availability of the system may be compromised. There is no documentation describing the required configuration of audit trails to record information to assist in intrusion detection. **Likelihood: HIGH** Without this documentation, the application of the audit security control may be applied inconsistently, incorrectly, or incompletely. **Impact: HIGH** Both intentional and unintentional human threats can cause damage to the system. Without proper audit log configuration and periodic audit log review, inappropriate system activity may not be detected. Exercise of this vulnerability could result in significant impairment to the SBE mission.		configuration of audit trails.
M-135	System security planning should address if the audit trails are used as online tools to help identify problems other than intrusions as they occur.	U	If system security planning does not address if the audit trails are used as online tools to help identify problems other than intrusions as they occur, then problems other than intrusions may go undetected or unresolved and the confidentiality, integrity, and availability	LOW	Consider documenting and implementing the use of online audit tools for identifying system problems, if cost effective.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			of the system may be compromised. There is no documentation addressing if the audit trails are used as online tools to help identify problems as they occur. Without online event log review, it is difficult to identify problems as they occur. **Likelihood: HIGH** There are no online event logs available on the server for review. **Impact: LOW** Because online event logs are not available to assist in problem identification, problem resolution may take longer to accomplish.		
M-136	System security planning should address if audit trails specify type of event, when the event occurred, user ID associated with the event, and program or command used to initiate the event.	U	If system security planning does not address if audit trails specify type of event, when the event occurred, user ID associated with the event, and program or command used to initiate the event, then audit trails may be incomplete and the confidentiality, integrity, and availability of the system may be compromised. There is no documentation to specify type of event, when the event occurred, user ID associated with the event, and program or command used to initiate the event. Without the ability to associate users with events accountability cannot	HIGH	Implement a formal and documented process describing the proper configuration of audit trails, specify the type of events to audit, when the event occurred, user ID associated with the event, and program or command used to initiate the event.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~be enforced.~~ ~~**Likelihood: HIGH**~~ ~~Without properly configured audit logs that are reviewed regularly, individual accountability for system actions can not be enforced.~~ ~~**Impact: HIGH**~~ ~~Both intentional and unintentional human threats can cause damage to the system. Without proper audit log configuration and periodic audit log review, inappropriate system activity may not be detected. Exercise of this vulnerability could result in significant impairment to the SBE mission.~~		
~~M-137~~	~~System security planning should address if access to electronic audit logs is strictly controlled.~~	~~U~~	~~If system security planning does not address if access to electronic audit logs is strictly controlled, then unauthorized access to electronic logs may occur resulting in the loss of audit trails and the confidentiality, integrity, and availability of the system may be compromised.~~ ~~There is no documentation addressing if access to electronic audit logs is strictly controlled. Without controlling access to the logs, they may be deleted either intentionally or unintentionally.~~ ~~**Likelihood: LOW**~~ ~~Other processes and controls, including~~	~~**LOW**~~	~~Implement a formal and documented process addressing access to electronic audit logs.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			physical isolation and small number of privileged users, reduces the likelihood of exploiting this vulnerability. **Impact: HIGH** If the audit logs are improperly modified or deleted, accountability for user actions cannot be enforced.		
M-138	System security planning should address if there exists separation of duties between security personnel who administer the access control function and those who administer the audit trail.	P	If system security planning does not address if there exists separation of duties between security personnel who administer the access control function and those who administer the audit trail, then a conflict of interest may exist whereby the audit trail can be circumvented resulting in the potential compromise of system confidentiality, integrity, and availability. Separation of Duties is practiced when possible due to the lack of resources at the SBE and LBEs, so most often the system administrator conducts both duties. **Likelihood: HIGH** A malicious administrator can exploit this vulnerability. **Impact: MEDIUM** Inappropriate activity may not be detected and losses may occur through a malicious administrator adding	**MEDIUM**	Implement a formal and documented process addressing how Separation of Duties is to be implemented.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			inappropriate users to the system without being detected.		
M-139	System security planning should address how confidentiality of audit trail information is protected.	U	If system security planning does not address how confidentiality of audit trail information is protected, then unauthorized access or modification to audit trails may occur resulting in the loss of the confidentiality of the audit trail information. There is no documentation addressing how confidentiality of audit trail information is protected. Without security controls implemented to identify fraudulent or erroneous changes to the system, it is difficult to identify when any improper use of the system has occurred, therefore audit trail data should remain confidential. **Likelihood: LOW** Other processes and controls, including physical isolation and small number of privileged users, reduces the likelihood of exploiting this vulnerability. **Impact: HIGH** Both intentional and unintentional human threats can cause damage to the system. Inappropriate activity may not be detected and significant losses may occur.	LOW	Implement a formal and documented process addressing how confidentiality of audit trail information is protected.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
M-140	System security planning should describe how frequently audit trails are reviewed and whether there are review guidelines.	U	If system security planning does not describe how frequently audit trails are reviewed and whether there are review guidelines, then audit trails may not be reviewed in a timely manner resulting in the failure to identify potential threats/vulnerabilities before they are exercised which may eventually lead to the compromise of the system confidentiality, integrity, and availability. There is no documentation describing how frequently audit trails are to be reviewed and there are no review guidelines. Without security controls implemented to identify fraudulent or erroneous changes to the system, it is difficult to identify when any improper use of the system has occurred, therefore audit trail data should remain confidential. **Likelihood: LOW** Other processes and controls, including physical isolation and small number of privileged users, reduces the likelihood of exploiting this vulnerability. **Impact: HIGH** Both intentional and unintentional human threats can cause damage to the system. Inappropriate activity may not be detected and significant losses may occur.	LOW	Implement a formal and documented process describing how frequently audit trails are reviewed.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
~~M-141~~	~~System security planning should address if the audit trails can be queried by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information.~~	~~M~~	~~The system documentation describes the process for reviewing event system logs by application name, date, time, user ID and terminal ID.~~		
~~M-142~~	~~System security planning should address if the appropriate system level or application level administrator reviews the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.~~	~~M~~	~~The Technicians Guide, GEMS Server Administrator Guide, and the RISC database describe the appropriate system level or application level administrator reviews the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.~~		
~~M-143~~	~~The System security planning should address the use of audit analysis tools.~~	~~U~~	~~If the System security planning does not address the use of audit analysis tools, then the audit analysis tools may be inappropriately used or deployed resulting in the failure to identify potential threats/vulnerabilities before they are exercised which may eventually lead to the compromise of the system confidentiality, integrity, and availability.~~ ~~Documentation does not address the use of audit analysis tools. Analyzing audit logs is a time consuming, labor intensive requirement, therefore audit analysis tools should be used.~~	~~LOW~~	~~Implement a formal and documented process addressing the use of audit analysis tools.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			Likelihood: LOW Other processes and controls, including physical isolation and small number of privileged users, reduces the likelihood of exploiting this vulnerability. **Impact: HIGH** Both intentional and unintentional human threats can cause damage to the system. Inappropriate activity may not be detected and significant losses may occur.		
M-144	Senior Management must assess and incorporate results of the risk assessment activity into the decision making process.	**M**	Results from this risk assessment will determine the effectiveness of existing security controls, provide recommendations, and establish baseline controls. Continue the risk assessment process at least every three years or whenever major changes occur throughout all phases of the system's life cycle.		
M-145	SBE should support or use the risk management process to identify and assess new potential risks and implement new security controls as needed to safeguard their IT systems.	**M**	Results from this risk assessment will determine the effectiveness of existing security controls, provide recommendations, and establish baseline controls. Continue the risk assessment process at least every three years or whenever major changes occur throughout all phases of the system's life cycle.		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~Note: This risk assessment is the first performed on the Accuvote-TS voting system.~~		
~~M-146~~	~~IT security trainers or security/subject matter professionals must understand the risk management process so that they can develop appropriate training materials and incorporate risk assessment into training programs to educate the end users.~~	~~M~~	~~The RISC Plan, SBE and LBE training manuals address the risk management process in regards to the training programs. Future training should place greater emphasis on the risk management process.~~		
~~M-147~~	~~To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system.~~	~~M~~	~~Results from this risk assessment will determine the effectiveness of existing security controls, provide recommendations, identify threats, and establish baseline controls.~~ ~~Note: This risk assessment is the first performed on the Accuvote-TS voting system.~~		
~~M-148~~	~~An estimate of the motivation, resources, and capabilities that may be required to carry out a successful attack should be developed after the potential threat-sources have been identified, in order to determine the likelihood of a threat exercising a system vulnerability.~~	~~M~~	~~Results from this risk assessment will determine the effectiveness of existing security controls, provide recommendations, assess threats, and establish baseline controls.~~ ~~Note: This risk assessment is the first performed on the Accuvote-TS voting system.~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
M-149	If the IT system has not yet been designed, the search for vulnerabilities should focus on the organizations security policies, planned security procedures, and system requirement definitions, and the vendors or developers security product analyses.	N/A	The system is not in the design phase.		
M-150	If the IT system is being implemented, the identification of vulnerabilities should be expanded to include more specific information, such as the planned security features described in the security design documentation and the results of system certification test and evaluation.	N/A	The system is not in the implementation phase.		
M-151	If the IT system is operational, the process of identifying vulnerabilities should include an analysis of the IT system security features and the security controls, technical and procedural, used to protect the system.	M	Results from this risk assessment will determine the effectiveness of existing security controls, provide recommendations, identify threats, and establish baseline controls. Note: This risk assessment is the first performed on the Accuvote-TS voting system.		
M-152	A cost-benefit analysis should be conducted for the proposed recommended controls, to demonstrate that the costs of implementing the controls can	M	The SBE RISC Plan addresses proposed recommended controls and provides justification and cost/benefit analysis information.		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	be justified by the reduction in the level of risk.				
M-153	The operational impact (e.g., effect on system performance) and feasibility (e.g., technical requirements, user acceptance) of introducing the recommended option should be evaluated carefully during the risk mitigation process.	M	The SBE RISC Plan addresses the operational impact and feasibility of introducing the recommended option and provides for careful evaluation during the risk mitigation process.		
M-154	Once the risk assessment has been completed (threat sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results should be documented in an official report or briefing.	M	This risk assessment documents the risks, effectiveness of existing security controls, provides recommendations, identifies threats, and establishes baseline controls. Note: This risk assessment is the first performed on the Accuvote-TS voting system.		
M-155	The goals and mission of an organization should be considered in selecting any risk mitigation options.	M	This risk assessment considers the goals and missions of SBE when suggesting risk mitigation options. In addition, the SBE RISC Plan ensures that the controls recommended by this risk assessment consider the goals and mission of the SBE.		
M-156	Priority should be given to the threat and vulnerability pairs that have the potential to cause significant mission impact or harm.	M	This risk assessment gives priority to the threat and vulnerability pairs that have the potential to cause significant mission impact or harm. Note: This risk assessment is the first performed on the Accuvote-TS voting		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~system.~~		
~~M-157~~	~~Ongoing risk management should be conducted to assess and mitigate risk.~~	~~M~~	~~The SBE RISC Plan ensures ongoing risk management is conducted to assess and mitigate risk.~~		
~~M-158~~	~~IT systems should be authorized to address and accept residual risk.~~	~~M~~	~~The SBE RISC Plan ensures that IT systems are authorized to operate and that residual risk is accepted.~~		
~~M-159~~	~~If the residual risk has not been reduced to an acceptable level, the risk management cycle must be repeated to identify a way of lowering the residual risk to an acceptable level.~~	~~M~~	~~The SBE RISC Plan ensures that residual risk is accepted or lowered to an acceptable level through the risk management cycle.~~		
~~M-160~~	~~There should be a specific schedule for assessing and mitigating mission risks~~	~~M~~	~~The SBE RISC Plan and the Change Control Plan have a specific schedule for accessing and mitigating risks.~~		
~~M-161~~	~~Risk management should identify residual risks for which contingency plans must be put into place.~~	~~M~~	~~The SBE Disaster Recovery and Incident Management Plan details the procedures to recover from a disaster/incident. This risk assessment identifies residual risks for which contingency plans must be put into place.~~		
~~M-162~~	~~SBE shall require that the system design should incorporate redundancy directly into the system architecture to optimize reliability, maintainability, and availability.~~	~~M~~	~~The system specifications incorporate redundancy directly into the system architecture to optimize reliability, maintainability, and availability.~~		
~~M-163~~	~~SBE shall have contingency test plans~~	~~M~~	~~The SBE Disaster Recovery and Incident Management Plan details the procedures~~		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~test plans.~~		~~Management Plan details the procedures for contingency test plans.~~		
~~M-164~~	~~The contingency plan should be updated to reflect changes to procedures based on lessons learned.~~	~~M~~	~~The SBE Disaster Recovery and Incident Management Plan and the Configuration Control Plan are updated based on lessons learned.~~		
~~M-165~~	~~The State Administrator shall maintain management control over the system and all support personnel provided by the system vendor.~~	~~M~~	~~The State Administrator maintains management control over the system and all support personnel as stated in the COMAR.~~		
~~M-166~~	~~SBE will ensure that any equipment within the control of a vendor for repairs, the equipment may not be used for voting or any election purposes.~~	~~M~~	~~The Election Judge manuals, SBE Maintenance Plan and the Election Administration Guide ensure that any equipment within the control of a vendor is not used for voting or any election purposes.~~		
~~M-167~~	~~Votes shall be recorded in audit trail memory, both in the voting unit and on the memory card, in two formats: as a summary total for each candidate and question, and as an individual ballot image of each voter's selection.~~	~~M~~	~~This voting system is compliant FEC standards. Votes are recorded in audit trail memory, both in the voting unit and on the memory card, in two formats: as a summary total for each candidate and question, and as an individual ballot image of each voter's selection as stated in the vendor guides.~~		
~~M-168~~	~~During post voting verification, if the verification does not agree with the original tabulation, the local board shall immediately notify the State Administrator.~~	~~M~~	~~As directed in COMAR, Election Administrators Guide and the Official Canvassing Guide local board shall immediately notify the State Administrator if the verification does not agree with the original tabulation.~~		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
~~M-169~~	~~The system and its components will only be used for conducting elections and may not be used for any other purpose.~~	~~M~~	~~The system and its components are only used for conducting elections and not used for any other purpose.~~		

Operational Controls

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
O-1	SBE will test electronic voting equipment for the proper implementation of state-specific requirements.	M	The SBE has User Acceptance Testing Guidelines in place to perform acceptance testing on all electronic voting equipment and UPS devices against state requirements. The SBE and LBE have AccuVote-TS Logic & Accuracy Testing in place to test the electronic voting equipment meets state requirements.		
O-2	SBE will define user acceptance testing for all electronic voting equipment.	M	The SBE has User Acceptance Testing Guidelines in place to perform acceptance testing on all electronic voting equipment and UPS devices against state requirements.		
O-3	SBE will ensure that a process is implemented that ensures that all voting devices shall record and retain redundant copies of the original ballot image.	M	SBE requires ITA certification, which ensures that all voting devices shall record and retain redundant copies of the original ballot image.		
O-4	SBE will ensure that a process is implement that protects against a single point of failure that would prevent further voting at the polling place.	M	The Election Judge manuals, AccuVote-TS – Technician's What If's, Technicians' Morning Checklist and SBE Procedures for Election Day establish processes to protect against a single point of failure.		
O-5	SBE will maintain a record, as required by law, (Federal and State) of all original audit data that cannot be modified or overridden but may be	M	A process is in place to maintain a record, as required law, Federal and State of all original audit data that cannot be modified or overridden but may be augmented by designated authorized		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~augmented by designated authorized officials in order to adjust for errors or omissions (e.g., during the canvassing process).~~		~~officials in order to adjust for errors or omissions (e.g., during the canvassing process) as defined in the Election Judges Manual.~~		
~~O-6~~	~~SBE will ensure that a process is implemented that detects and records every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator.~~	~~M~~	~~The AccuVote-TS and GEMS software both detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator as described in Precinct Count 1.96 User's Guide, AccuVote System Guide and GEMS 1.18 User Guide to conform to state requirements in COMAR 33.10.02.10~~		
~~O-7~~	~~SBE will ensure that a process is implemented that maintains a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path.~~	~~M~~	~~The Procedures for Official Canvas, Verification and Post-Election Audit, Recount procedures; GEMS 1.18 Users Guide, and Election Judges Guide ensure a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path is maintained.~~		
~~O-8~~	~~SBE will ensure that a process is implemented to retrieve ballot images in a form readable by humans.~~	~~M~~	~~The Election Judges Guide describes the process that is used to ensure the ballot image is in a form readable by humans.~~		
~~O-9~~	~~SBE will ensure that all error messages requiring intervention by an operator or precinct~~	~~M~~	~~The Precinct Count 1.96 User's Guide covers all error messages requiring intervention by an operator or precinct~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	official shall be displayed or printed unambiguously in easily understood language text, or by means of other suitable visual indicators.		official displayed or printed is unambiguously in easily understood language text, or by means of other suitable visual indicators.		
O-10	SBE will ensure that a process is implemented for a security seal, a password, or a data code recognition capability to prevent the inadvertent or unauthorized actuation of the DRE Device.	P	If SBE does not ensure that a process is implemented for a security seal, a password, or a data code recognition capability to prevent the inadvertent or unauthorized actuation of the DRE device, then integrity of the DRE device may not be maintained resulting in the potential loss of system confidentiality, integrity, and availability. The AccuVote-TS Pre-Election Logic & Accuracy Testing and Checklist procedures ensure a security seal is placed on each DRE device. However, the key used to lock the PCMCIA card and printer on the DRE has a universal key (i.e., the same key for all DREs). **Likelihood: MEDIUM** With the number of Diebold DRE devices on the market it is likely that a key could become lost or stolen. However, the openness of the polling stations impedes the exploitation of this vulnerability. **Impact: MEDIUM** The impact of the exploitation of this vulnerability could impact multiple DRE devices, adversely impacting SBE's	**MEDIUM**	The key used to lock the PCMCIA card and the printer should be specific to individual DRE devices or groups of DRE devices or tamper-proof tape should be placed over the lock and/or access panel during the election.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			~~mission.~~		
~~O-11~~	~~SBE will implement procedures to establish and maintain controls that ensure that accidents, inadvertent mistakes, and errors are minimized.~~	~~M~~	~~The Technicians Election Day Check Lists; Tech's TS What If's; SBE Procedures for Election Day, and Election Judges Guidelines have been implemented to establish and maintain controls that ensure that accidents, inadvertent mistakes, and errors are minimized.~~		
~~O-12~~	~~SBE will implement procedures to protect the system from intentional manipulation and fraud, and from malicious mischief.~~	~~M~~	~~The AccuVote-TS Pre-Election Logic & Accuracy Testing and Checklist, Technicians Election Day Check Lists; Tech's TS What If's; SBE Procedures for Election Day, and Election Judges Guidelines have been implemented to establish and maintain controls that ensure effective procedures to protect the system from intentional manipulation and fraud, and from malicious mischief are followed.~~		
~~O-13~~	~~SBE will implement procedures to protect secrecy in the voting process.~~	~~M~~	~~The Election Judge and Polling officials follow procedures in the Election Judge's Manual to protect secrecy in the voting process.~~ ~~AccuVote-TS also ensures privacy because it does not use personal information.~~		
~~O-14~~	~~SBE will implement procedures to prevent unauthorized~~	~~P~~	~~If SBE does not implement procedures to prevent unauthorized changes to system~~	~~HIGH~~	~~SBE should replace the public FTP server with Secure Copy (SCP), Secure FTP~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	changes to system capabilities for defining ballot formats, casting and recording votes, calculating vote totals consistent with defined ballot formats, and reporting vote totals.		capabilities for defining ballot formats, casting and recording votes, calculating vote totals consistent with defined ballot formats, and reporting vote totals, then system confidentiality, integrity, and availability may be compromised. The AccuVote-TS Logic and Accuracy Testing procedures have been implemented to prevent unauthorized changes to system capabilities for defining ballot formats, casting and recording votes, calculating vote totals consistent with defined ballot formats, and reporting vote totals; however during the Ballot Creation Process the ballot is transferred to the LBEs via an FTP server. **Likelihood: HIGH** The ballot format can be modified either while in transit or while on the public FTP server. **Impact: HIGH** An attacker could use this server to change the initial ballot and possibly place Trojan software within the ballot data causing the validity and integrity of the election to be questioned. An FTP server is one of the most insecure ways to distribute files.		(sFTP), Secure Sockets Layer (SSL), or Transport Layer Security (TLS) to protect the ballot during transmission. SBE should encrypt the ballot while on the intermediate server to prevent unauthorized access to the file.
O-15	SBE will implement procedures to prevent the changing or	M	The Election Judge and Polling officials follow procedures in the Election Judge's		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~prevention of recording a vote.~~		~~Manual to prevent the changing or prevention of recording a vote. The DRE only allows the voter to cast one vote. Once a vote is cast, the Voter Access Card is deactivated and cannot be used again until reactivated by the election officials.~~		
~~O-16~~	~~SBE will implement procedures to prevent changing calculated vote totals.~~	~~M~~	~~The Election Judge and Polling officials follow procedures in the Election Judge's Manual to prevent changing calculated vote totals. The LBE officials follow Election Results Transfer Memorandum to prevent changing calculated vote totals. The SBE officials follow Election Results Transfer Memorandum and General Election Night Processing procedures to prevent changing calculated vote totals.~~		
~~O-17~~	~~SBE will implement procedures to prevent access to vote data, including individual votes and vote totals, to unauthorized individuals.~~	~~M~~	~~The Election Judges, Polling officials and technicians follow procedures in Technicians Election Day Check Lists; Tech's TS What If's, SBE Procedures for Election Day, and Election Judges Guidelines to prevent access to vote data, including individual votes and vote totals, to unauthorized individuals.~~		
~~O-18~~	~~SBE will implement a process to prevent access to voter identification data for votes cast by the voter such that an individual can determine the content of specific votes casts by the voter.~~	~~M~~	~~The Election Judges Manual establishes a process to prevent access to voter identification data for votes cast by the voter such that an individual can determine the content of specific votes casts by the voter.~~ ~~AccuVote-TS also ensures privacy~~		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~because it does not use personal information.~~		
~~O-19~~	~~SBE will implement procedures that require all systems that transmit data over public telecommunications networks to preserve the secrecy of a voter's ballot choices, and prevent anyone from violating ballot privacy.~~	~~M~~	~~As certified by the ITA, the DRE does not transmit individual ballot information.~~		
~~O-20~~	~~SBE will implement procedures that detect the occurrence of a telecommunication interruption at the poll site and switch to an alternative mode of operation that is not dependent on the connection between the poll site voting devices and external system components.~~	~~M~~	~~The Elections Judges Manual and Election Administrator's Guide establishes procedures to detect the occurrence of a telecommunication interruption at the poll site and switch to an alternative mode of operation that is not dependent on the connection between the poll site voting devices and external system components.~~		
~~O-21~~	~~SBE will implement procedures to provide an alternate voting mode without the voter losing their ability to vote.~~	~~M~~	~~The provisional ballot process outlined in the Election Judges Manual provides an alternate voting mode without the voter losing their ability to vote.~~		
~~O-22~~	~~Emergency procedures should be put in place for contingencies such as equipment failure or malicious activity that could make the voting systems unavailable.~~	~~M~~	~~The SBE Disaster Recovery and Incident Management Plan are in place for contingencies such as equipment failure or malicious activity that could make the voting systems unavailable.~~		
~~O-23~~	~~SBE shall implement procedures that will protect the DRE units from unauthorized~~	~~N/A~~	~~The DRE voting terminals are not connected to communications lines during the election.~~		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~access via communications lines.~~		~~during the election.~~		
~~O-24~~	~~SBE shall implement procedures that will protect the DRE units from unauthorized access via wireless communications.~~	~~N/A~~	~~The DRE units are not connected to wireless communications.~~		
~~O-25~~	~~All electronic information shall be backed up as appropriate and secured from unauthorized access.~~	~~M~~	~~All electronic information is backed up where appropriate and secured from unauthorized access as defined in the Election Judges Manual and the State-Wide Voting System Project General Election Results Export Procedures.~~		
~~O-26~~	~~Upon learning of a possible incident, SBE needs to take steps to verify that the incident actually does exist.~~	~~M~~	~~Upon learning of a possible incident, the SBE follows steps within the Disaster Recovery and Incident Management Plan to verify that the incident actually does exist.~~		
~~O-27~~	~~Once the incident is verified, its scope should be determined.~~	~~M~~	~~Once the incident is verified, its scope is determined by following the Disaster Recovery and Incident Management Plan.~~		
~~O-28~~	~~When apprising users of the existence of an incident, SBE should make every attempt to provide clear and concise information.~~	~~M~~	~~When apprising users of the existence of an incident, SBE follows the Disaster Recovery and Incident Management Plan to make every attempt to provide clear and concise information.~~		
~~O-29~~	~~SBE must accurately record and report the defects in vendor-provided software products to the proper vendors~~	~~M~~	~~The Quality Assurance (QA) Plan and Risks, Issues, Systems Incidents, and Changes (RISC) Plan accurately record and report the defects in vendor-provided~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	~~and, to user groups. The reports must be held confidential and reported to the proper vendor(s) in a timely manner.~~		~~software products to the proper vendors and, to user groups. The reports held confidential and reported to the proper vendor(s) in a timely manner.~~		
~~O-30~~	~~SBE shall comply with all intellectual property, copyright, patent, or trade secret issues.~~	~~M~~	~~SBE complies with all intellectual property, copyright, patent, or trade secret issues as stated in the contract with vendor.~~		
~~O-31~~	~~If SBE possesses source code or has made non-disclosure agreements, care should be taken to avoid revealing any information that is legally protected.~~	~~N/A~~	~~The SBE does not possess source code. SBE complies with non-disclosure agreements.~~		
~~O-32~~	~~Incident logging should be treated much the same as evidence gathering: the incident log should be detailed, accurate, and the proper procedures should be followed so that the incident log could be used as evidence in a court of law.~~	~~U~~	~~If incident logging is not treated the same as evidence gathering, then legal requirements for chain of custody may not be met resulting in the inability to prosecute and/or unrecoverable financial loss.~~ ~~SBE does not have detailed evidence gathering procedures or processes.~~ ~~**Likelihood: LOW**~~ ~~The possibility of an attacker to gain access to a DRE source code for malicious activity is unlikely in its current configuration. The possibility of an attacker to gain access to a GEMS server for malicious activity is also~~	~~**LOW**~~	~~Establish procedures to preserve the incident logs on the DREs and the GEMS server and incorporate additional logging so that these logs may be used as evidence in a court of law.~~

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~unlikely in its current configuration.~~ ~~**Impact: LOW**~~ ~~Although incident logging is performed on the DREs and the GEMS server, there are no procedures established regarding these incident logs so they could be used as evidence in a court of law.~~		
~~O-33~~	~~After an incident has been resolved, a review should be conducted so that SBE can learn from the experience and, if necessary, update its procedures.~~	~~M~~	~~The Disaster Recovery and Incident Management Plan covers the process after an incident has been resolved, regarding reviews and updates to procedures.~~		
~~O-34~~	~~The security features of an IT system must be configured (e.g., enabled or disabled) to meet the needs of a specific installation and to account for changes in the operational environment.~~	~~U~~	~~If the security features of an IT system are not configured (e.g., enabled or disabled) to meet the needs of a specific installation and to account for changes in the operational environment, then security controls may be applied inconsistently or circumvented and the confidentiality, integrity, and availability of the system may be compromised. Some of the security services of the IT system are provided by the software itself. Buffer overflows and unchecked file locations could provide system level access to the OS.~~ ~~The following software vulnerabilities were found in the AccuVote-TS voting system source code.~~	~~**MEDIUM**~~	~~For the memcpy, tcscpy sscanf, and lstrcpy functions, ensure that the bounds of the receiving buffers are checked before the operation begins, and that operations cease when the buffer is full.~~ ~~Use more secure functions to acquire random numbers, such as mt_rand, which is faster than the average libc and can be used with cryptography.~~ ~~Declare necessary variables as constant to ensure that they could not be changed by malicious activities.~~ ~~When creating static arrays and variable declarations, ensure that the size allocated is larger than the maximum~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			The memcpy, tcscpy, sscanf, and lstrcpy functions do not check the size of the receiving variable, making them vulnerable to a buffer overflow. The srand function is not secure in its implementation of acquiring random numbers. Sprintf and vsprintf formatting is not declared as a constant, which would prevent changes to a variable. There are many static variable declarations used which could be utilized in a buffer overflow. No paths were used to designate external library files, allowing possible trojans to be introduced. The system function is used which allows for shell execution of the passed parameter. The crypt function is used for a one-way hash, this function is vulnerable to a dictionary based, brute force attack. Race conditions exist for temporary file accesses, this could allow for a file substitution which could lead to unauthorized access. The open function is used to open files. This does no checking for valid files, and		possible length. Specify paths to external library files by using registry entries or other verifiable system variables. Do not use shell execution methods without extensive checking of the passed parameter to defend against trojaned operation. The crypt function is an outdated method for creating a cryptological hash. Use SHA-1 for a more secure hash. Race conditions can be avoided programmatically so that no two calls reference the same resource at the same time. Perform validation checking before doing any file operations.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			symlinks or shortcuts could be used to open device files or data outside the scope of this function. **Likelihood: MEDIUM** These findings are mitigated by the fact that the DREs are not connected to a network and by the openness of the voting environment. **Impact: HIGH** An attacker could use these vulnerabilities to gain full access to the voting system, invalidating any other security controls, and allowing access to the or possible alteration of the voting results.		
O-35	It is essential to detect security breaches (e.g., network break-ins, suspicious activities) so that a response can occur in a timely manner.	U	If security breaches (e.g., network break-ins, suspicious activities) are not detected so that a response can occur in a timely manner, then mitigation efforts may be after-the-fact resulting in loss of system confidentiality, integrity, and availability. SBE does not detect security breaches. **Likelihood: HIGH** SBE currently has a GEMS server used to generate and distribute ballots with no security mechanisms in place. The ballots are distributed to the LBEs for proofing and Logic and Accuracy Testing	**HIGH**	Remove the SBE GEMS server from network and rebuild entire system from trusted media to assure and validate system has not been compromised. Do not put any software other than the GEMS software on the system. Locate the server in a secure location.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~before the election; however the Logic and Accuracy Testing does not role the date ahead to check for Trojan software.~~ ~~**Impact: HIGH**~~ ~~An attacker could use this server to change the initial ballot and possibly place a Trojan software within the ballot data.~~		
~~O-36~~	~~Security responsibility should be assigned to ensure that adequate security is provided for the mission-critical IT systems.~~	~~M~~	~~The Election Judge Manual and the Technician Guide assign responsibility to ensure that adequate security is provided for the mission-critical IT systems. This function is performed by LBE and precinct staff.~~		
~~O-37~~	~~Personnel security controls, including separation of duties, least privilege, and user computer access registration and termination should be implemented.~~	~~M~~	~~The Election Judges Manual, and Election Administrator's Guide establishes personnel security controls, including separation of duties, least privilege, and user computer access registration and termination. This function is performed by LBE and precinct staff.~~		
~~O-38~~	~~Security awareness and technical training should be conducted to ensure that end users and system users are aware of the rules of behavior and their responsibilities in protecting the organizations mission. This training will include information about threats, risks and vulnerabilities~~	~~U~~	~~If security awareness and technical training is not conducted to ensure that end users and system users are aware of the rules of behavior and their responsibilities in protecting the organization's mission, then security controls may be applied inconsistently or circumvented and the confidentiality, integrity, and availability of the system may be compromised.~~	~~**HIGH**~~	~~Training should be established for security awareness and technical training to ensure that system users are aware of the rules of behavior and their responsibilities in protecting the organizations mission. This training should include information about threats, risks, vulnerabilities, and risks to voting systems.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	to voting systems, and the need to protect them.		may be compromised. Security awareness and technical training is not conducted to ensure that end users and system users are aware of the rules of behavior and their responsibilities in protecting the organizations mission. The SBE has training for all of the election judges, poll workers and technicians. However, this training does not adequately address security issues. **Likelihood: HIGH** Without security awareness training the election judges, poll workers and technicians may not be aware of their security responsibilities. **Impact: HIGH** If the vulnerability is exploited the validity and integrity of the election process may be compromised.		
O-39	Periodic testing of security controls should be conducted to ensure that the controls are effective.	U	If periodic testing of security controls is not conducted to ensure that the controls are effective, then unplanned risks may be introduced to the system and the existing security controls may be circumvented and the confidentiality, integrity, and availability of the system may be compromised. Periodic security testing is not performed	**LOW**	Implement a periodic security testing program to ensure that the system security controls remain effective over time.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			for the AccuVote-TS voting system. **Likelihood: LOW** The risk assessment process is an effective control for baselining the existing security controls and the system risks. **Impact: HIGH** If the vulnerability is exploited the validity and integrity of the election process may be compromised.		
O-40	Periodic system audits should be performed.	M	Periodic system audits are performed using the Logic and Accuracy Plan and the Procedures for Official Canvass, Verification and Post-Election Audit.		
O-41	Continuity of support should be provided, and a continuity of operations plan should be developed, tested, and maintained to provide for business resumption and ensure continuity of operations during emergencies or disasters.	M	A Continuity of Operations plan has been developed, tested, and maintained in the Disaster Recovery and Incident Management Plan and the Emergency Continuity Plan. An inventory of backup DREs is maintained at the LBE. The SBE maintains a backup GEMS server at the State of Maryland Archives building. In addition, Diebold has a warehouse of DRE devices located at BWI airport.		
O-42	An incident response capability should be developed to prepare for, recognize, report, and respond to the incident and return the IT system to operational status.	M	The Disaster Recovery and Incident Management Plan and the Emergency Continuity Plan establish an incident response capability to prepare for, recognize, report, and respond to the incident and return the IT system to		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~operational status.~~		~~operational status.~~		
~~O-43~~	~~To ensure consistency and uniformity in security operations, step-by-step procedures and methods for implementing (preventive and detection) operational controls must be clearly defined, documented, and maintained.~~	~~U~~	~~If step-by-step procedures and methods for implementing (preventive and detection) operational controls are not clearly defined, documented, and maintained, then security controls may be applied inconsistently or circumvented and the confidentiality, integrity, and availability of the system may be compromised.~~ ~~No security operations, step-by-step procedures and methods for implementing (preventive and detection) operational controls is defined, documented, and maintained. Therefore, operational controls may be implemented inconsistently, incorrectly, and incompletely. Interviews with system personnel indicated that security functions were being performed.~~ ~~**Likelihood: LOW**~~ ~~The absence of consistent and uniform security controls may lead to unauthorized, undetected, or unknown changes to system settings. This vulnerability can be exploited by all human threats, but due to other existing physical and technical security controls this has been rated low.~~ ~~**Impact: HIGH**~~ ~~The exploitation of a GEMS server may~~	~~**LOW**~~	~~To ensure consistency and uniformity in security operations, step-by-step procedures and methods for implementing (preventive and detection) operational controls must be clearly defined, documented, and maintained by the SBE and LBE.~~

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~cause the validity and integrity of the voting process to be compromised.~~		
~~O-44~~	~~The person responsible for voting system contingency planning must be aware of risks to the system and recognize whether the current contingency plan is able to address residual risks completely and effectively.~~	~~M~~	~~The personnel responsible for voting system contingency planning are aware of risks to the system and recognize whether the current contingency plan is able to address residual risks completely and effectively as shown in the Emergency Contingency Plan and the Disaster Recovery and Incident Management Plan.~~		
~~O-45~~	~~There should be coordination between each IT Contingency plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.~~	~~N/A~~	~~There are no interconnections to other systems. Therefore, there is not a requirement for coordination between multiple contingency plans.~~		
~~O-46~~	~~Organizations should prepare their internal and external communications procedures prior to a disaster.~~	~~M~~	~~The SBE has an established Disaster Recovery and Incident Management Plan and Emergency Contingency Plan.~~		
~~O-47~~	~~Contingency measures should be identified and integrated at all phases of the computer system life cycle.~~	~~M~~	~~The Risks, Issues, System Incidents and Changes (RISC) Plan and SBE AccuVote Touch Screen Voting System, Phase II Implementation Plan satisfy contingency measures identified and integrated at all phases of the computer system life cycle.~~		
~~O-48~~	~~Contingency planning requirements should be considered when a new~~	~~M~~	~~SBE AccuVote Touch Screen Voting System, Phase II Implementation Plan has procedures for risk management~~		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~process is being conceived.~~		~~planning identification to be considered.~~		
~~O-49~~	~~Contingency strategies should be tested (in the implementation phase) to ensure that technical features and recovery procedures are accurate and effective. Testing on an ongoing basis, as necessary, shall be conducted to ensure that procedures continue to be effective.~~	~~N/A~~	~~The system is not in the implementation phase.~~		
~~O-50~~	~~Backups should be stored offsite.~~	~~U~~	~~If backups are not stored offsite, then a disaster may destroy both the original and backup data copy making system recoverability difficult or impossible.~~ ~~The systems, PCMCIA cards, and paper backups are all stored at the same location. Therefore, a disaster at the storage facility could destroy all the voting records from the election.~~ ~~**Likelihood: LOW**~~ ~~Existing physical controls at the storage facility mitigate the likelihood.~~ ~~**Impact: LOW**~~ ~~The canvassing process is completed prior to the final storage of the PCMCIA cards and paper backups, therefore the impact of the loss would be minimal.~~	~~**LOW**~~	~~Implement a procedure for storing backups offsite.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
O-51	When the IT system undergoes upgrades or any other modifications, such as changes to external interfaces, these modifications should be reflected in the contingency plan, in a timely manner.	M	The Disaster Recovery and Incident Management Plan has procedures to reflect upgrades and any other modifications, such as changes to external interfaces to the DRE and GEMS server.		
O-52	Until a new system is operational and fully tested (including its contingency capabilities), the original system's contingency plan should be ready for implementation.	N/A	The AccuVote-TS voting system is in the operational and maintenance phase of its life cycle. It is not undergoing replacement.		
O-53	The contingency planning policy statement should define the SBE's overall contingency objectives and establish the organizational framework and responsibilities for IT contingency planning.	M	The Disaster Recovery and Incident Management Plan defines the SBE's overall contingency objectives and establish the organizational framework and responsibilities for IT contingency planning.		
O-54	SBE officials must support the Contingency Planning process and should be included in the process to develop the program policy, structure, objectives, and roles and responsibilities.	M	SBE officials support the Contingency Planning process and have been included in the process to develop the program policy, structure, objectives, and roles and responsibilities.		
O-55	As the IT contingency policy and program are developed, they should be coordinated with related SBE activities, including IT security, physical security,	M	The IT contingency policy and program are developed, and are coordinated with related SBE activities, including IT security, physical security, human resources, IT operations, and emergency		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~human resources, IT operations, and emergency preparedness functions.~~		~~preparedness functions.~~		
~~O-56~~	~~Contingency plans must be written in coordination with other existing plans associated with systems.~~	~~M~~	~~Contingency plans have been written in coordination with other existing plans associated with the system.~~		
~~O-57~~	~~Preventive controls should be documented in the contingency plan, and personnel associated with the system should be trained on how and when to use the controls.~~	~~M~~	~~Preventive controls are documented in the Election Judge Manual, and personnel associated with the system are trained on how and when to use the controls.~~		
~~O-58~~	~~Preventive controls should be maintained in good condition to ensure their effectiveness in an emergency.~~	~~M~~	~~Preventive controls are maintained in good condition to ensure their effectiveness in an emergency.~~		
~~O-59~~	~~Procedures should specify the frequency of backups (e.g., daily or weekly, incremental or full), based on data criticality and the frequency that new information is introduced.~~	~~M~~	~~The Election Judges Manual and General Election Results Export Procedures provides steps for backups of data.~~		
~~O-60~~	~~Data backup documentation should designate the location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite.~~	~~M~~	~~The Election Judges Manual and General Election Results Export Procedures designate the location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite.~~		
~~O-61~~	~~The specific method chosen for conducting backups should be~~	~~M~~	~~The Election Judges Manual and General Election Results Export~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	based on system and data availability and integrity requirements.		Procedures establish several methods to backup the data, including hard copy, magnetic media and central standalone server.		
O-62	The contingency plan must include a strategy to recover and perform system operations at an alternate facility for an extended period.	M	The Disaster Recovery and Incident Management Plan and Emergency Contingency Procedure include a strategy to recover and perform system operations at an alternate facility for an extended period.		
O-63	The alternate facility chosen must be able to support system operations as defined in the contingency plan.	M	The Disaster Recovery and Incident Management Plan and Emergency Contingency Procedure choose alternate facilities capable to support system operations as defined in the contingency plan.		
O-64	Alternate site selection of fixed-site locations should account for the time and mode of transportation necessary to move personnel there.	M	The Disaster Recovery and Incident Management Plan and Emergency Contingency Procedure take into account for the time and mode of transportation necessary to move personnel there when selecting an alternate site selection.		
O-65	The alternate fixed site should be in a geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure) as the organization's primary site.	M	The Disaster Recovery and Incident Management Plan and Emergency Contingency Procedure considers geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure) as the organization's primary site when choosing an alternate site.		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
O-66	Contingency test results and lessons learned shall be documented and reviewed by test participants and other personnel as appropriate.	M	The Disaster Recovery and Incident Management Plan and Emergency Contingency Procedure has established process for contingency testing and lessons learned.		
O-67	A copy of the contingency plan shall also be stored at the alternate site and with the backup media.	M	Each LBE as well as the SBE has a copy of the Disaster Recovery and Incident Management Plan and Emergency Contingency Procedure.		
O-68	The Contingency Planning Coordinator should maintain a record of copies of the plan and to whom they were distributed.	U	If the Contingency Planning Coordinator does not maintain a record of copies of the plan and to whom they were distributed, then outdated plans may be in circulation, which may impact recovery in the event of a disaster. A record of copies of the plan and to whom they were distributed is not maintained. Therefore it is possible for outdated plans to remain in circulation. **Likelihood: LOW** A small number of officials are responsible for coordinating contingency plans are their implementation. These responsible individuals are in constant communication during an election. **Impact: LOW** Activation of contingency plan could be delayed because the contingency planning coordinator may have an	**LOW**	A record of copies of the contingency plan should be maintained by SBE and LBE.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~outdated contact list.~~		
~~O-69~~	~~Other information that should be stored with the contingency plan includes contracts with vendors (SLAs and other contracts), software licenses, system users' manuals, security manuals, and operating procedures.~~	~~M~~	~~Along with the contingency plan, LBEs have copies of the relevant documentation and produced the documentation on request.~~		
~~O-70~~	~~The Contingency Planning Coordinator should record plan modifications using a Record of Changes, which lists the page number, change comment, and date of change.~~	~~M~~	~~The Risks, Issues, Systems Incidents, and Changes (RISC) Plan is used to record plan modifications.~~		
~~O-71~~	~~The Contingency Planning Coordinator should coordinate frequently with associated internal and external organizations and system POCs to ensure that impacts caused by changes within either organization will be reflected in the contingency plan.~~	~~M~~	~~The Disaster Recovery and Incident Management Plan has established a requirement to update plan at least once a year. As part of this update, the Contingency Planning Coordinator interacts with internal and external organizations and POCs.~~		
~~O-72~~	~~Strict version control must be maintained.~~	~~M~~	~~The Disaster Recovery and Incident Management Plan has strict version control implemented.~~		
~~O-73~~	~~The Contingency Planning Coordinator should evaluate supporting information to ensure that the information is~~	~~M~~	~~The Disaster Recovery and Incident Management Plan has procedures to evaluate supporting information to ensure that the information is current and~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	current and continues to meet system requirements adequately.		continues to meet system requirements adequately.		
O-74	Damage assessment procedures should be developed for the voting system.	M	The Disaster Recovery and Incident Management Plan has procedures to assess the damage of the voting system.		
O-75	Personnel with damage assessment responsibilities should understand and be able to perform these procedures in the event the paper plan is unavailable during the situation.	M	Election Judges and system technicians, who have damage assessment responsibilities, are given training to understand and be able to perform these procedures in the event the paper plan is unavailable during the situation.		
O-76	The IT contingency plan should be activated by the appropriate authority only when the damage assessment indicates that one or more of the activation criteria for that system are met.	M	The Disaster Recovery and Incident Management Plan has an escalation procedure and activation criteria determined by the damage assessment results.		
O-77	Teams with recovery responsibilities should understand and be able to perform these recovery strategies well enough that if the paper plan is unavailable during the initial stages of the event, they can still perform the necessary activities.	N/A	This requirement is outside of the scope of this assessment. If teams with recovery responsibilities do not understand and are not able to perform these recovery strategies well enough that if the paper plan is unavailable during the initial stages of the event, then plan execution may be incomplete or inaccurate.		
O-78	Recovery procedures should reflect system priorities	U	If recovery procedures do not reflect system priorities identified in the	LOW	Ensure the Business Impact Analysis (BIA) identifies critical IT resources, single

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	identified in the Business Impact Analysis.		Business Impact Analysis, then critical systems may not be recovered first. A Business Impact Analysis identifies system priorities and the impact they have on the voting process. A Business Impact Analysis has not been performed. **Likelihood: LOW** Other system controls such as the Disaster Recovery and Incident Response Plan list recovery priorities. **Impact: LOW** Recovery priorities may not be optimized.		points of failure, internal and external POC associated with the system, develops recovery priorities, and determines disruption impacts and allowable outage times. Ensure procedures for identifying, selecting, installing, and modifying system software are also addressed by the BIA.
O-79	The contingency plan should provide detailed procedures to restore the IT system or system components. To prevent difficulty or confusion in an emergency, no procedural steps should be assumed or omitted	M	The Disaster Recovery and Incident Management Plan have established procedures to restore the IT system or system components. To prevent difficulty or confusion in an emergency, no procedural steps are assumed or omitted.		
O-80	Procedures should be assigned to the appropriate recovery team.	M	The Disaster Recovery and Incident Management Plan has established recovery team assignments.		
O-81	Until the primary system is restored and tested, the contingency system should continue to be operated.	M	The Disaster Recovery and Incident Management Plan has procedures to continue the use of contingency system.		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
O-82	The Reconstitution Phase should specify teams responsible for restoring or replacing both the site and the IT system.	M	The Disaster Recovery and Incident Management Plan has established procedures on System and Facility Recovery.		
O-83	In addition to backing up data, organizations should also back up system device drivers.	U	If in addition to backing up data, organizations do not also back up system device drivers, then systems may not be fully recoverable. Backup of device drivers is not performed. When device drivers are not backed up, restoration of the system is impeded. **Likelihood: LOW** The likelihood of needing device driver backups is low because the device drivers are contained in the OS. **Impact: LOW** The impact is low because the device drivers can be restored from the OS.	LOW	Backup device drivers in addition to other data.
O-84	It is important that media be retrieved on a regular basis from off-site storage and tested to ensure that the backups are being performed correctly.	N/A	Data is only stored as required by law for post election audit and challenges to an election (maximum of 22 months).		
O-85	Each backup tape, cartridge, or disk should be uniquely labeled, including a date, to ensure that the required data can be	N/A	Data is only stored as required by law for post election audit and challenges to an election (maximum of 22 months).		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	the required data can be identified quickly in an emergency.				
O-86	If remote access is established as a contingency strategy: (1) Data bandwidth requirements should be identified and used to scale the remote access solution; (2) Security controls such as one-time passwords should be considered; and, (3) Data encryption should be implemented if the communications contains sensitive information.	N/A	Remote access is not supported in the contingency strategy.		
O-87	Security patches should be tested to check for any unintended consequences on configuration or software specific to the organization.	M	The ITA recertifies any patches or upgrades of the systems. An Acceptance and Accuracy Test and Certification are then performed by the SBE and the LBE performs a Logic and Accuracy Test and Certification before the patches or upgrades are accepted for use.		
O-88	All unneeded default accounts and groups should be removed to eliminate their use by intruders, including guest accounts on computers containing sensitive information.	M	All unneeded default accounts and groups are removed to eliminate their use by intruders, including guest accounts on computers containing sensitive information. Needed default accounts are in use and should be closed and replaced with non-		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			default accounts.		
O-89	To prevent alteration of executable code, no software shall be permanently installed or resident in the system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware.	U	If the alteration of executable code is allowed, then unplanned risks may be introduced to the system and the existing security controls may be circumvented and the confidentiality, integrity, and availability of the system may be compromised. SBE receives all software and firmware and software directly from the ITA. SBE, in turn, instructs the vendor what version to load on systems. With this arrangement, the vendor can load uncertified software on to the system without SBE's knowledge. **Likelihood: HIGH** The vendor has a contractual obligation to load only certified software, but there are no controls to ensure this occurs. **Impact: HIGH** An uncertified version may contain malicious code, which could compromise the integrity of the voting process.	**HIGH**	SBE should verify correct firmware and software version prior to use.
O-90	After initiation of election day testing, no source code or compilers or assemblers shall be resident or accessible on the voting system.	M	The ITA has verified no source code or compilers or assemblers shall be resident or accessible on the voting system.		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
O-91	System and procedures must ensure that each voter can vote only once.	M	The Logic and Accuracy Test and Certification procedures check that each voter can vote only once. Also, the DRE only allows the voter to cast one vote. Once a vote is cast, the Voter Access Card is deactivated and can not be used again until reactivated by the election officials.		
O-92	End user access to the system is provided only through the approved interface.	M	The Election Judge Manual sets procedures for voter access to the system is provided only through the approved interface. The voter must verify their identity by the Book Election Judge and be given a Voter Authority Card before allowed access to the Voting Unit Access Judge. Once the voter is at the Voting Unit Access Judge, the voter must relinquish his Voter Authority Card and receive an activated Voter Access Card. The voter interfaces with the DRE voting terminal only through the touch screen interface. The DRE does not have any infrared ports or exposed communications ports to facilitate unauthorized access to the terminal.		
O-93	Process is in place to apply appropriate security patches to maintain a secure configuration.	U	If processes are not in place to apply appropriate security patches to maintain a secure configuration, then the existing security controls may be circumvented and the confidentiality, integrity, and availability of the system may be compromised. A process is not in place to apply	**MEDIUM**	Create and implement a formal process to ensure that the voting system is up to date with all applicable patches.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~security patches in order to maintain a secure configuration.~~ ~~**Likelihood: MEDIUM**~~ ~~Implementation of security patches ensures system stability and availability. Two high vulnerabilities were discovered on the GEMS server, however due to the existing operational and physical security controls this risk likelihood is rated medium.~~ ~~**Impact: HIGH**~~ ~~A malicious user could use these vulnerabilities to gain complete system control either locally or remotely. Additionally, without these security patches, the system may become unavailable.~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
O-94	Voters must be authenticated to the system, using established procedures.	M	Election Judges' Manual establishes procedures to authenticate voters to the DRE as directed in Election Law Article, § 10-310		
O-95	A post election audit must be conducted in order to reconcile and ensure that the number of voters equals the number of votes, and the votes were accurately collected.	M	Procedures for Official Canvass, Verification and Post-Election Audit are conducted in order to reconcile and ensure that the number of voters equals the number of votes, and the votes were accurately collected. Note: Only 10% validation is currently performed and actual transmissions become official record after canvassing. We recommend the canvassing of 100% of the precincts once the DRE is deployed statewide. The time to perform a 100% is minimal and would validate pre-election testing.		
O-96	SBE will ensure that, local LBE election boards conduct and document Logic and Accuracy Tests of every DRE voting terminal prior to election day.	M	Each LBE conducts Logic and Accuracy Test and Certification on each DRE voting terminal.		
O-97	SBE will ensure that, local election boards conduct and document a system verification test on every voting unit within.	M	Each LBE conducts Logic and Accuracy Test and Certification on each DRE voting terminal.		
O-98	SBE will ensure that the system shall permit voting in secrecy.	M	The Election Judge and Polling officials follow procedures in the Election Judge's Manual to protect secrecy in the voting process. The DRE voting terminals block		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	taking the signed VAC to the next step in the voting process.		and instruct the voter on taking the signed VAC to the next step in the voting process. These VAC cards are used to verify the vote totals at the conclusion of the election against the vote totals stored in the DRE memory. Also if a DRE were damaged or destroyed during an election such that the vote data for votes already cast could not be retrieved from the machine, the State of Maryland could use the VACs for that machine to contact the affected voters to have them return to the polling station and recast their votes. The next step in the voting process is for the voter to present his or her VAC to the election official responsible for the DRE terminal. The election official takes the voter's VAC and activates a DRE Voter Access Card smartcard for that voter. The election official places the VAC in the envelop associated with the DRE terminal and permits the voter to insert the DRE Voter Access Card smartcard into the DRE to vote.		
O-104	Local election boards will ensure that the judges manual provides detailed poll closing procedures including: a) How to document public and protective counter totals; b) How to end the election; c) How to print and sign the vote total reports; d) How to post the vote totals reports; e) How to remove the memory cards from the voting	M	The judges manual provides detailed poll closing procedures including: a) How to document public and protective counter totals; b) How to end the election; c) How to print and sign the vote total reports; d) How to post the vote totals reports; e) How to remove the memory cards from the voting units; f) How to return the materials to the local board office.		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	units; f) How to return the materials to the local board office.				
O-105	If a consolidation of memory cards is used, the Election Judges shall perform the consolidation in accordance with the election judges manual.	M	According to interviews with Election Judges, they perform the consolidation and verification of the vote totals in accordance with the Election Judge Manual.		
O-106	Local boards shall develop and SBE shall approve procedures for returning priority items to the local board after closing the election.	M	Each LBE has procedures for returning priority items to the local board after closing the election in the Election Judge Manual to prevent high priority items from being lost or stolen.		
O-107	Local boards shall develop and SBE shall approve procedures for aggregating precinct counts which will include written procedures for: a) Assembling memory cards from each polling place; b) Transferring votes from the memory cards to the EMS; c) Manually entering absentee ballot results into the EMS; d) Aggregating vote counts for the entire county; e) Securing the physical area where the tabulation takes place; f) Controlling access to the area, including documentation for who may be admitted to the area, by name or job function.	M	Each LBE Election Judge Manual has procedures approved by the SBE to: a) Assembling memory cards from each polling place; b) Transferring votes from the memory cards to the EMS; c) Manually entering absentee ballot results into the EMS; d) Aggregating vote counts for the entire county; e) Securing the physical area where the tabulation takes place; f) Controlling access to the area, including documentation for who may be admitted to the area, by name or job function.		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
~~O-108~~	~~Local boards shall develop and SBE shall approve procedures for tabulation of write-in votes which: a) In a general election, the results report produced by the voting unit shall indicate the number of votes cast in each write-in position for each contest; b) The results memory card shall contain the names of individuals for whom voters cast write-in votes and shall copy those names to the EMS; c) Require the production of a printed report of all write-in votes, which shall be tallied, recorded, and reported.~~	~~M~~	~~The Ballot Creation Process establishes the ballot to include write-in votes. The Logic and Accuracy Test and Checklist is used to verify the tabulation of the write-in votes prior to each election.~~		
~~O-109~~	~~On completion of pre-election testing, the local board shall secure master copies of the ballot control logic in a secure, locked location, designated by the local board, but separate from the location of the working copies. They shall be retained as required by law, court order, or SBE directive.~~	~~M~~	~~The LBE securely stores a master copy of the ballot separate from the location of the working copies.~~		
~~O-110~~	~~The local board shall develop a plan for retaining and storing memory cards, consolidation reports and other data processing materials related to the election. The plan shall be consistent with the Election~~	~~M~~	~~Each LBE retains and stores memory cards, consolidation reports and other data processing materials related to the election, consistent with the Election Records Management Program and approved by the State Administrator. Storage of this information is in a secure~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	Records Management Program and be approved by the State Administrator. Storage shall be in a locked location and for such time until the period for challenging the election expires and for any additional time required by law or Regulation.		location and is retained for such time until the period for challenging the election expires and for any additional time required by law or Regulation.		

~~Technical Controls~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
~~T-1~~	~~To ensure vote accuracy, SBE will ensure that all systems include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy.~~	~~U~~	~~If SBE does not ensure that all systems include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy, then the data could be modified or deleted when transmitted and system integrity would be compromised.~~ ~~The PCMCIA flash memory card used to store the election results does not contain any cryptographic hashes that could be used to verify the data integrity before and after transmission and verification.~~ ~~**Likelihood: LOW**~~ ~~Based on the existing security control of manual data reconciliation, there is little danger of data corruption becoming a critical issue.~~ ~~**Impact: MEDIUM**~~ ~~If data is modified or deleted during submission, there is no automated parity checking, and it becomes necessary to use manual reconciliation, then the time allowed for vote tallying could greatly increase.~~	~~**LOW**~~	~~Perform automated cryptographic hash creation once data is entered, then check that hash once the data has been transmitted to the destination.~~

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
~~T-2~~	~~To ensure vote accuracy, SBE will ensure that all systems provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected.~~	~~M~~	~~All of the system functions are logged whenever an action occurs during setup as well as during normal operation.~~		
~~T-3~~	~~SBE will ensure that a consolidated printed report of the results for each contest of all votes cast that includes the votes cast for each selection, the count of undervotes, and the count of overvotes is produced.~~	~~M~~	~~The DRE voting machines print out a report of the results of each station during the post-election using the internal printing device. This report includes the votes cast for each selection, the count of undervotes, and the count of overvotes.~~		
~~T-4~~	~~SBE will ensure controls are implemented to ensure that there is no access path from unofficial electronic report or files to the storage devices for official data.~~	~~M~~	~~SBE has documented procedures that require the transfer of data from the DRE voting machine to the GEMS server only occur while the DREs are in the same physical location, or utilize point-to-point communications.~~		
~~T-5~~	~~SBE will ensure controls are implemented to clearly indicate on each unofficial report or file that the results it contains are unofficial.~~	~~M~~	~~SBE has processes in place to ensure controls are implemented to clearly indicate on each unofficial report or file that the results it contains are unofficial.~~		
~~T-6~~	~~SBE will ensure security controls are implemented to identify fraudulent or erroneous changes to the system.~~	~~U~~	~~If SBE does not ensure security controls are implemented to identify fraudulent or erroneous changes to the system, then it is very difficult to identify when any improper use of the system has occurred~~	~~HIGH~~	~~Windows 2000 OS on the GEMS server should be configured to audit all security events that are generated. These logs should be reviewed on a regular basis, archived for future use, and protected~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			improper use of the system has occurred and system integrity may be compromised. **Likelihood: HIGH** Audit logs on the GEMS server are not configured to log any security events, or any extended system information. **Impact: HIGH** Both intentional and unintentional human threats can cause damage to the system, and no audit records are stored to determine if damage occurred.		archived for future use, and protected from unauthorized disclosure. Additionally, administrative user accounts should not be shared by multiple users.
T-7	SBE will ensure security controls are implemented to prevent alteration of voting system audit trails.	M	The voting system software only allows users with a Supervisor card to purge log entries and backup data.		
T-8	SBE will ensure security controls are implemented to prevent introduction of data for a vote not cast by a voter.	M	If SBE does not ensure security controls are implemented to prevent introduction of data for a vote not cast by a voter, then the vote data would be inaccurate and system integrity would be compromised. Only voters with a valid Voter Access Card can cast votes.		
T-9	SBE will ensure security controls are implemented that require all systems that transmit data over public	U	If SBE does not ensure security controls are implemented that require all systems that transmit data over public telecommunications networks to employ	**HIGH**	The DRE voting terminal should contain a cryptographic signature that is unique to each terminal. Cryptographic signatures, those based on a session identifier, rather

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~telecommunications networks to employ digital signature for all communications between the vote server and other devices that communicate with the server over the network.~~		~~digital signature for all communications between the vote server and other devices that communicate with the server over the network, then the data sent from a DRE voting terminal cannot be positively identified as valid data and system integrity may be compromised.~~ ~~Digital signatures are not used to protect and verify the integrity of the election data while it is in transit over the public switched telephone network.~~ ~~**Likelihood: HIGH**~~ ~~In order to exploit this vulnerability, a malicious threat source would need to have knowledge of the particular telecommunications network on which this data would be traveling and the ability to intercept the traffic without either end noticing interception.~~ ~~**Impact: HIGH**~~ ~~If a malicious threat source were able to compromise the data in transit, then they would be able to substitute invalid data for valid data, causing inaccurate results for the election.~~		~~than a static ID, are difficult to forge and should be used.~~
~~T-10~~	~~SBE will ensure security controls are implemented that require all systems that transmit data over public telecommunications networks to require that at least two~~	~~M~~	~~In order to process ballots, both the DRE voting terminal and the GEMS server must be in the mode to do so, which requires a Supervisor Access Card for the terminal, and administrator login rights for the GEMS software. Those~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	authorized election officials activate any critical operation regarding the processing of ballots.		rights are only given to authorized election officials, each of whom adheres to the two officials rule.		
T-11	SBE will implement security controls to create and preserve an audit trail of every vote cast during the period of interrupted communication and system operation.	M	All of the voting terminals have an internal battery that powers the system in the event of power loss, and there is an Uninterruptible Power Supply (UPS) for the GEMS server that tallies votes, as well. If the DRE voting terminal had communication problems, the data is stored on a non-volatile flash memory card. Even once the card is reset for a new election, a backup file is kept on the card unless purged by a Supervisor Access Card. Any ballot that was created but does not have any results transmitted after an election close will be flagged by the GEMS software.		
T-12	Anti-virus tools should be used to detect, identify, or remove viruses.	U	If anti-virus tools are not used to detect, identify, or remove viruses, then there could be serious threats to the availability of the voting service. There is no anti-virus software installed on the GMES voting server. **Likelihood: MEDIUM** Although neither the DRE voting terminal nor the LBE GEMS servers will be connected to any publicly available network, it is possible that during system updates, viruses could be introduced to	**MEDIUM**	Ensure that anti-virus software is used on the GEMS voting server, and that anti-virus definition files are updated regularly.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~the system.~~ ~~**Impact: HIGH**~~ ~~A virus could cause problems as severe as data corruption and data deletion on both the DRE voting terminals and the GEMS servers.~~		
~~T-13~~	~~Systems should implement DAC or MAC.~~	~~M~~	~~Both the GEMS server and the DRE voting terminals practice discretionary and mandatory access controls over the data.~~		
~~T-14~~	~~Cryptographic keys must be securely managed when cryptographic functions are implemented in various other controls. (Cryptographic key management includes key generation, distribution, storage, and maintenance).~~	~~N/A~~	~~Cryptographic keys are not used in the AccuVote-TS voting machines.~~		
~~T-15~~	~~Organization IT systems and networks that employ routable protocol devices shall contain intrusion detection systems (IDS).~~	~~P~~	~~If IDS systems are not installed to detect network intrusions and potential breaches in progress, then unauthorized access may be undetected and information may be modified and deleted resulting in the potential loss of confidentiality, integrity, and availability of system data.~~ ~~The LBE GEMS voting server and the DRE voting are not connected to a publicly available network that might contain an external interface that would~~	~~**HIGH**~~	~~Remove the SBE GEMS server from network and rebuild entire system from trusted media to assure and validate system has not been compromised. Do not put any software other than the GEMS software on the system. Locate the server in a secure location.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			necessitate the use of IDS. The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. **Likelihood: HIGH** SBE currently has a GEMS server used to generate and distribute ballots with no security mechanisms in place. The ballots are distributed to the LBEs for proofing and Logic and Accuracy Testing before the election; however the Logic and Accuracy Testing does not role the date ahead to check for Trojan software. **Impact: HIGH** An attacker could use this server to change the initial ballot and possibly place a Trojan software within the ballot data.		
T-16	IDS systems shall be installed with boundary protection devices (e.g., firewalls) and/or routers to detect network intrusions and potential breaches in progress at all points external to the SBE network and when the risk analyses dictate an IDS on internal networks.	N/A	The LBE GEMS voting server and the DRE voting are not connected to a publicly available network that might contain an external interface that would necessitate the use of IDS. The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. This risk is analyzed in requirement T-15.		
T-17	IDS systems shall be installed on voting system collection	N/A	The LBE GEMS voting server and the DRE voting are not connected to a		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	server to detect intrusions.		publicly available network that might contain an external interface that would necessitate the use of IDS. The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. This risk is analyzed in requirement T-15.		
T-18	SBE networks shall be protected by boundary protection devices (firewalls and trusted guards) at identified points of interface with lesser or unsecured networks. These security devices and configurations shall be designed and implemented employing a system security engineering/risk management process.	N/A	The LBE GEMS voting server and the DRE voting are not connected to a publicly available network that might contain an external interface that would necessitate the use of firewalls. The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. This risk is analyzed in requirement T-15.		
T-19	Firewalls shall define and implement a network security policy based on an engineering/risk management process.	N/A	The LBE GEMS voting server and the DRE voting are not connected to a publicly available network that might contain an external interface that would necessitate the use of firewalls. The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. This risk is analyzed in requirement T-15.		
T-20	Firewalls shall block all services not required and disable unused ports.	N/A	The LBE GEMS voting server and the DRE voting are not connected to a publicly available network that might contain an external interface that would		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~necessitate the use of firewalls.~~ ~~The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. This risk is analyzed in requirement T-15.~~		
~~T-21~~	~~Firewalls shall hide and prevent direct accessing of Department trusted network addresses from untrusted networks.~~	~~N/A~~	~~The LBE GEMS voting server and the DRE voting are not connected to a publicly available network that might contain an external interface that would necessitate the use of firewalls.~~ ~~The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. This risk is analyzed in requirement T-15.~~		
~~T-22~~	~~Firewalls shall maintain comprehensive audit trails.~~	~~N/A~~	~~The LBE GEMS voting server and the DRE voting are not connected to a publicly available network that might contain an external interface that would necessitate the use of firewalls.~~ ~~The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. This risk is analyzed in requirement T-15.~~		
~~T-23~~	~~Firewalls shall fail in a closed state.~~	~~N/A~~	~~The LBE GEMS voting server and the DRE voting are not connected to a publicly available network that might contain an external interface that would necessitate the use of firewalls.~~ ~~The SBE GEMS server is connected to the SBE Intranet, which has access to~~		

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			the Internet. This risk is analyzed in requirement T-15.		
T-24	Firewalls shall operate on a dedicated platform (device).	N/A	The LBE GEMS voting server and the DRE voting are not connected to a publicly available network that might contain an external interface that would necessitate the use of firewalls. The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. This risk is analyzed in requirement T-15.		
T-25	Downloading of mobile code and executable content from a controlled interface between interconnected systems shall be permitted only when a boundary protection device appropriately configured (to handle such a download) is in place and approved by the SBE.	N/A	The LBE GEMS voting server and the DRE voting are not connected to a publicly available network. The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. This risk is analyzed in requirement T-15.		
T-26	Operating systems should be configured to set ACLs/Permissions for system files, administrative tools, system registry entries, and files that control security services in applications.	M	The voting server has the appropriate ACLs/Permissions for system files for the system files, administrative tools, system registry entries, and files that control security services in applications.		
T-27	Operating systems should be configured to enforce password history to 24 passwords remembered.	U	If operating systems are not configured to enforce password history to 24 passwords remembered, then users could recycle commonly used	**MEDIUM**	Configure the GEMS voting server to enforce password history to 24.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	remembered.		passwords, thereby reducing the effective security of those passwords and system integrity may be compromised. The GEMS voting server does not enforce password history. **Likelihood: MEDIUM** Access to the GEMS server is limited. **Impact: HIGH** This vulnerability could be exploited by a malicious insider gaining knowledge of a valid user's password that was required to be changed, but was then changed back to the original password. This could allow unauthorized users access to the sensitive voting data.		
T-28	Operating systems should be configured to set minimum password age to 1 day and maximum password age to 90 days.	U	If operating systems are not configured to set minimum password age to 1 day and maximum password age to 90 days, then password controls may be ineffective and it may be possible for unauthorized users to gain access to privileged data and system integrity may be compromised. Operating systems are not configured to set minimum password age to 1 day and maximum password age to 90 days. Passwords should not be changed too rapidly, or some users will set a newly changed password to one they have used previously. The longer a password	**MEDIUM**	Configure the GEMS voting server to enforce a minimum password age of 1 day and a maximum password age of 90 days.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~is used the more likely it is that the password will be intercepted by a malicious user.~~ ~~The GEMS voting server does not enforce minimum or maximum password age.~~ ~~**Likelihood: HIGH**~~ ~~Effective password controls are not currently in place.~~ ~~**Impact: HIGH**~~ ~~If a malicious insider were to intercept or acquire a valid user's password, they could gain access to privileged data.~~		
~~T 29~~	~~Only administrators should have the ability to add, change, or remove system or application level files.~~	~~M~~	~~The users profile for the GEMS voting server have the appropriate access controls set for the system files, administrative tools, system registry entries, and files that control security services in applications.~~		
~~T 30~~	~~Operating systems should be configured to lock the desktop of the current user after fifteen minutes of inactivity and to lock out the account of any user that has three invalid login attempts.~~	~~U~~	~~If operating systems are not configured to lock the desktop of the current user after fifteen minutes of inactivity and to lock out the account of any user that has three invalid login attempts, then it is possible for the user to walk away and leave the server open for some other person to use. Not having an account become locked after 3 tries makes it much easier for passwords to be guessed. System confidentiality,~~	~~**HIGH**~~	~~Set the default screensaver timeout to 15 minutes and to require a password to unlock. Set the account lockout policy to deny access after 3 failed attempts.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			integrity, and availability may be compromised. The GEMS voting server does not have a desktop timeout set, nor does it lock an account after 3 failed login attempts. **Likelihood: HIGH** The controls are not effective to prevent a motivated threat source from exploiting this vulnerability. The lack of a session timeout and unlimited login attempts, coupled with the fact that the auditing control is not effectively utilized result in a high likelihood that this vulnerability would be exploited. **Impact: HIGH** If a malicious user were to access a computer that was left unlocked by a valid user, then they would have access to the same resources and data that user normally has. Without an account lockout count, then a malicious user can use a brute-force attack to guess a user's password, again gaining access to the valid user's resources and data.		
T 31	In low-risk environments, the event logs should be used weekly to review the log files; in higher risk environments, log files should be reviewed daily when in operation.	U	If event logs are not regularly reviewed, then it is very difficult to identify when any improper use of the system has occurred and system confidentiality and integrity may be compromised. Event logs on the server are not	HIGH	Event logs should be reviewed on a regular basis.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			reviewed on a regular basis. **Likelihood: HIGH** Without event log review, inappropriate activity may not be detected. **Impact: HIGH** Both intentional and unintentional human threats can cause damage to the system and without audit log review, inappropriate system activity may not be detected. Exercise of this vulnerability could result in significant impairment to the SBE mission.		
T-32	The "Require logon to change the password" parameter is required so that users are logged on a system before they can change their password. If a password has expired and the users are currently not logged on a system, a System Administrator (SA) must log on to change the user password.	M	Users must logon to the system to change their password or have the System Administrator change their password if they are not logged on and their password is expired.		
T-33	Passwords should meet State of Maryland Security Standards.	U	If passwords do not meet State of Maryland Security Standards, then easily guessable passwords may allow unauthorized access to the system resulting in the potential loss of confidentiality, integrity, and availability. Passwords are not required to have any	**HIGH**	Create a local security policy that enforces the password security policies of the State of Maryland. Ensure that the passwords are properly configured on all voting system components.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			password complexity or minimum length. **Likelihood: HIGH** Effective password controls are not currently in place. **Impact: HIGH** A malicious user could guess passwords and possibly gain the ability to take over and replace processes, and access other computers on the network.		
T-34	System should be configured to prompt user to change password 14 days before its expiration.	N/A	Passwords are not currently set to expire.		
T-35	Maximum log size should be set to record all necessary events or comply with local logging policy and installed hardware limitations.	U	If the maximum log size is not set to record all necessary events or comply with local logging policy and installed hardware limitations, then it is possible that events that were not reviewed would be deleted in order to reuse space and audit trails would be lost. The maximum log size for Windows 2000 GEMS server was set to 512 kilobytes and events to be overwritten after 7 days. This is insufficient to trace events that could cause problems with the voting system. **Likelihood: HIGH** This control is not effective for retaining	**HIGH**	Set the maximum log to an appropriate size.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			system and security events pertinent to the voting system. **Impact: HIGH** Without a large enough maximum log size, an attacker or malicious user could generate a large number of system events, causing log entries to be overwritten. Exercise of this vulnerability could result in significant impairment to the SBE mission.		
T-36	Appropriate encryption software should be used for protecting sensitive information on a mobile computer/laptop.	N/A	No mobile computers or laptops are used as part of the voting system.		
T-37	Use of encryption is required when sensitive information is transmitted over an un-trusted public network domain (e.g., the Internet).	N/A	The LBE GEMS voting server and the DRE voting are not connected to a publicly available network. The SBE GEMS server is connected to the SBE Intranet, which has access to the Internet. This risk is analyzed in requirement T-15. It should be noted, that FTP is used; see O-14; modem transmissions are used; see T-42 below.		
T-38	System accounts will not be shared.	U	If system accounts are shared, it is not possible to trace events to individuals and system confidentiality, integrity, and availability may be compromised.	**HIGH**	Require that all system users have their own accounts.

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
			~~System accounts are shared.~~ ~~**Likelihood: HIGH**~~ ~~Systems accounts are shared. There are no other accounts on the machine beside the administrator, AccuVote, and accutouch accounts. Each user that is authorized for the machine should have their own account to ensure accountability.~~ ~~**Impact: HIGH**~~ ~~If a malicious user gains access to a shared system account, it would be very difficult to trace the actions of a legitimate system user versus those of the malicious user. Exercise of this vulnerability could result in significant impairment to the SBE mission.~~		
~~T 39~~	~~All system access by privileged users will be logged by the system.~~	~~U~~	~~If all system access by privileged users is not logged by the system, then it is not possible to trace events to individuals and system confidentiality, integrity, and availability may be compromised.~~ ~~Audit logs on the server are not configured to log security events.~~ ~~**Likelihood: HIGH**~~ ~~Without auditing privileged user access, inappropriate activity may not be detected.~~	~~**HIGH**~~	~~Windows 2000 Server should be configured to audit all security events that are generated.~~

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			Impact: HIGH Both intentional and unintentional human threats can cause damage to the system and without audit log review, inappropriate system activity may not be detected. Exercise of this vulnerability could result in significant impairment to the SBE mission.threats can cause damage to the system, and no audit records are stored to determine if damage occurred.		
T-40	The system bootstrap, monitor, and device-controller software may be resident permanently as firmware, provided that this firmware has been shown to be inaccessible to activation or control by any means other than by the authorized initiation and execution of the vote-counting program, and its associated exception handlers.	M	The firmware cannot be updated by any process from the voting server or the voting terminal itself.		
T-41	The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as computer chip) other than the component on which the operating system resides.	M	On the voting terminals, the operating system is located internally, while the election information is located both internally and on a removable PCMCIA flash memory card.		
T-42	Cryptography should be considered for data that is	U	If cryptography is not used for data that is sensitive, has a high value, or	HIGH	Implement cryptographic protocols for the data while it is transit such as hardware

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
	sensitive, has a high value, or represents a high value if it is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage.		represents a high value if it is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage, then data in transit and data at rest may be subject to unauthorized access and the confidentiality, integrity, and availability of the data may be compromised. Although the data is transmitted over a private point-to-point network, no cryptography is used to ensure the integrity of the data being passed. **Likelihood: HIGH** A motivated threat source could intercept the unencrypted data in transit. Access to communications closets at polling places, such as public schools, is not likely to be highly secured. **Impact: HIGH** A malicious user could intercept the data and modify it or copy it during transmission.		link-layer encryption (encrypting modems using 3DES or better encryption) or application-layer encryption (Secure Sockets Layer [SSL], Transport Layer Security [TLS], etc.).
T-43	Individual ballot images in memory must be randomized to protect voter secrecy.	U	If individual ballot images in memory are not randomized to protect voter secrecy, then it is possible to tie votes back to specific individuals and system confidentiality may be compromised. Individual ballots are stored sequentially.	**LOW**	Implement a function to randomize the write location of the individual ballot images.

Number	Baseline Security Requirements	M/P/U /NA	Likelihood/Impact or Existing Controls	Risk Rating	Mitigation Strategy
			Likelihood: LOW The likelihood is remote that individual vote records could be reconstructed due to the amount of collusion required to exploit this vulnerability. **Impact: LOW** The impact is low because it would affect a limited number of voters.		
T-44	SBE will ensure that voting units be maintained such that the voting mechanism can not be reopened to voting after: a) The manager card is inserted in to the card reader; b) The election judge's PIN number is entered on the screen; c) The "End Election" button is pressed.	M	SBE has processes in place to prevent the voting terminal from being reopened once the close of voting has taken place.		
T-45	SBE will ensure that the Election Management System shall tabulate and report the total votes cast for each candidate and for or against each question by precinct and by groups of precincts, such as districts, wards and countywide.	M	The State of Maryland has implemented a process to ensure that COMAR is adhered to for voting system integrity. COMAR requires tabulation and reporting of the total votes cast for each candidate and for or against each question by precinct, and by groups of precincts, such as districts, wards and countywide.		
T-46	SBE will ensure that the Election Management System shall tabulate and report total	M	SBE has implemented a Logic and Accuracy Test to ensure that COMAR is adhered to for voting system integrity		

~~Number~~	~~Baseline Security Requirements~~	~~M/P/U /NA~~	~~Likelihood/Impact or Existing Controls~~	~~Risk Rating~~	~~Mitigation Strategy~~
	~~votes cast in each contest and write-in voting positions.~~		~~and for each contest and write-in voting positions.~~		
~~T-47~~	~~SBE will ensure that local election boards conduct, as part of the pre-election testing, a public demonstration, as described in COMAR 33.10.02.16 .~~	~~M~~	~~The LBE has implemented a public demonstration to ensure that COMAR 33.10.02.16 is met.~~		

APPENDIX A: ACRONYMS

The following table contains acronyms used in the AccuVote-TS risk assessment report.

ACRONYM	MEANING
ACL	Access Control Lists
C&A	Certification and Accreditation
CIO	Chief Information Officer
COMAR	Code of Maryland Regulations
COOP	Continuity of Operations
DES	Data Encryption Standard
DoS	Denial of Service
DNS	Domain Name Server
DR	Disaster Recovery
DRE	Direct Recording Equipment
EMS	Election Management System
FEC	Federal Election Commission
GSS	General Support System
IDS	Intrusion detection system
IT	Information Technology
ITA	Independent Testing Authority
LBE	Local Board of Elections
NIST	National Institute of Standards and Technology
POC	Point of Contact
RA	Risk Assessment

ACRONYM	MEANING
SAIC	Science Applications International Corporation
SBE	State Board of Elections
ST&E	Security Test and Evaluation
UPS	Uninterrupted Power Source
WAN	Wide Area Network

APPENDIX B: SECURITY STATEMENTS FROM THE RUBIN REPORT & STATE OF MARYLAND CONTROLS

The following table is a brief analysis of statements made by Professor Rubin, et al, in their report on the Diebold source code entitled "Analysis of an Electronic Voting System", July 23, 2003. In general, SAIC made many of the same observations, *when considering only the source code.* While many of the statements made by Mr. Rubin were technically correct, it is clear that Mr. Rubin did not have a complete understanding of the State of Maryland's implementation of the AccuVote-TS voting system, and the election process controls or environment. During this assessment, SAIC had access to system and election documentation, personnel and equipment. Applying the NIST Risk Assessment methodology to the evaluation of the equipment in its operational environment and the totality of the management, operational, and technical controls, SAIC reached many different conclusions. Indeed, Professor Rubin states repeatedly in his paper that he does not know how the system operates in an election and he further identifies the assumptions that he used to reach his conclusions. In those cases where these assumptions concerning operational or management controls were incorrect, the resultant conclusions were, unsurprisingly, also incorrect.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
2	*"The anonymity of a voter's ballot must be preserved, both to guarantee the voter's safety when voting against a malevolent candidate, and to guarantee that voters have no evidence that proves which candidates received their votes."*	O-18, 0-19, T-43	The anonymity of a voter's ballot is preserved because the AccuVote-TS voting system does not use or store personal information and does not provide an individual paper record for each voter, therefore leaving no evidence of a single voter's selections. ~~The individual ballots however, are stored sequentially. If someone kept track of all of the individuals who voted on a particular DRE and then was able to obtain that system's PCMCIA card they would be able to tie votes back to individuals.~~
2	*"The voting system must also be tamper-resistant to thwart a wide range of attacks, including ballot stuffing by voters and incorrect tallying by insiders."*	M-4, M-5, O-91	The AccuVote-TS voting system only allows a voter to cast their vote one time. After the individual votes, the Voter Access Card is deactivated. In addition, there are physical, and procedural controls at the polling stations to ensure that voters are only given access to the DRE one time and to make sure that they do not vote multiple times. In addition, when the vote is cast by the voter, the Voter Access Card automatically ejects making a loud noise and the DRE is

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
			disabled until another valid Voter Access Card is inserted.
2	*"A voting system must be comprehensible and usable by the entire voting population, regardless of age, infirmity, or disability."*	N/A	This is not a security requirement.
2	*"The only known solution to this problem is to introduce a "voter-verifiable audit trail." [DMNW03]. Most commonly, this is achieved by adding a printer to the voting terminal. When the voter finishes selecting candidates, a ballot is printed on paper and presented to the voter. If the printed ballot reflects the voter's intent, the ballot is saved for future reference. If not, the ballot is mechanically destroyed. Using this "Mercuri method," [Mer00] the tally of the paper ballots takes precedence over any electronic tallies. As a result, the correctness of the voting terminal software no longer matters; either a voting terminal prints correct ballots or it is taken out of service."*	M-1, M-18, M-90, O-40	The AccuVote-TS voting system requires that the voter verify their selections prior to the actual casting of the vote. This is done via a review screen on the DRE. The AccuVote-TS voting system does not provide a paper "voter-verifiable audit trail" specific to individual voters. Note: A printed paper ballot would still be subject to fraud. A compromised machine could be programmed to record votes incorrectly, but provide a correct paper ballot to the voter. Only in the event of a total recount would this be discovered. Additionally, the process of hand counting the millions of votes is time consuming and is prone to error.
4	*"Most notably, voters can easily program their own smartcards to simulate the behavior of valid smartcards used in the election."*	M-1, M-5, M-83, O-91	Although it is possible for someone to buy and to program their own smartcard, the attacker would be limited to changing their party affiliation in the case of a primary (i.e., they could see a ballot meant for another party) because the smartcard only contains party affiliation and access to vote on the DRE. The combination of logic controls in the DRE software, the physical controls and the openness of the voting booths minimize the likelihood of the voter being able to cast multiple votes without being detected.
4	*"With such homebrew cards, a voter can cast multiple ballots without leaving any trace."*	M-1, M-5, O-91	Although it is possible for someone to buy and to program their own smartcard, the attacker would be limited to changing their party affiliation in the case of a primary (i.e., they could see a ballot meant for another party) because the smartcard only contains party affiliation and access to vote on the DRE. The combination of logic controls in the DRE software, the physical controls and the openness of the voting booths minimize the likelihood of the voter being able

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
			to cast multiple votes without being detected.
4	*"A voter can also perform actions that normally require administrative privileges, including viewing partial results and terminating the election early."*	M-88, O-12, O-14, 0-91,	A voter would need to manufacture a smartcard with administrator rights to obtain these privileges. Assuming someone could manufacture the card and obtained access to the DRE, the specific DRE device could be disabled (i.e., close election). Such an attack would be detected due to the physical controls and the openness of the voting booths. The Disaster Recovery and Incident Management Plan guide provides procedures for handling a disabled DRE.
4	*"Similar undesirable modifications could be made by malevolent poll workers (or even maintenance staff) with access to the voting terminals before the start of an election."*	M-1, M-13, M-26, O-37	The physical controls prevent any single individual from having access to the DRE devices prior to the election. The DRE devices are tested at the LBE warehouse, then sealed with tamper-proof tape prior to shipment to the polling site. The Election Judges remove the tamper-proof tape the morning of the election.
4	*"Furthermore, the protocols used when the voting terminals communicate with their home base, both to fetch election configuration information and to report final election results, do not use cryptographic techniques to authenticate the remote end of the connection nor do they check the integrity of the data in transit."*	M-18, M-41, O-14	The AccuVote-TS voting system is not using a modem to fetch election information. The results of the election however are transmitted. These transmissions are not encrypted. SAIC has recommended that these transmissions be encrypted and that a 100% verification of the transmissions and the PCMCIA cards occur.
4	*"Given that these voting terminals could communicate over insecure phone lines or even wireless Internet connections, even unsophisticated attackers can perform untraceable "man-in-the-middle" attacks."*	N/A	The DRE devices are not connected to a network. The DRE Accumulator is connected via modem after the election to transmit vote totals to the LBE. These transmissions are not encrypted and could be intercepted or modified. SAIC has recommended that these transmissions be encrypted and that a 100% verification of the transmissions and the PCMCIA cards occur.
4	*"Cryptography, when used at all, is used incorrectly."*	M-41, M-124, T-42	Currently, ~~DES~~ encryption is only used for the resident memory on the DRE in accordance with Federal requirements. Once the DRE is powered down, the resident memory is erased. SAIC has recommended that encryption

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
			be employed for the modem transmission of the vote totals.
4	*"In many places where cryptography would seem obvious and necessary, none is used."*	M-41, M-124, T-42	Currently, ~~DES~~ encryption is only used for the resident memory on the DRE. Once the DRE is powered down, the memory is erased. SAIC has recommended that encryption be employed for the modem transmission of the vote totals.
4	*"More generally, we see no evidence of rigorous software engineering discipline. Comments in the code and the revision change logs indicate the engineers were aware of areas in the system that needed improvement, though these comments only address specific problems with the code and not with the design itself."*	M-102, O-72, T-6	The scope of the risk assessment did not include a review of Diebold's software engineering practices. SAIC's review of the source code also noted similar comments. It should be noted that since the publication of the Rubin report, Diebold has developed, documented, and implemented a change control process, which has been delivered to the SBE.
4	*"We also saw no evidence of any change control process that might restrict a developer's ability to insert arbitrary patches to the code."*	M-102, O-72, T-6	The scope of the risk assessment did not include a review of Diebold's software engineering practices. It should be noted that since the publication of the Rubin report, Diebold has developed, documented, and implemented a change control process, which has been delivered to the SBE. SBE and LBE's Logic & Accuracy tests verify that votes are recorded accurately prior to the use of the DRE for any election. SAIC has also recommended that SBE enhance the controls for certifying that the implemented source code is the same version as that certified by the ITA, and to expand their testing to include testing for time-oriented exploits (e.g., trojans). This may be accomplished by changing the machine date and time to correspond to that of the election during testing.
4	*"Absent such processes, a malevolent developer could easily make changes to the code that would create vulnerabilities to be later exploited on Election Day."*	M-10, O-72, T-6	The scope of the risk assessment did not include a review of Diebold's software engineering practices. It should be noted that since the publication of the Rubin report, Diebold has developed, documented, and implemented a change control process, which has been delivered to the SBE. SBE and LBE's Logic & Accuracy tests verify that votes are

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
			recorded accurately prior to the use of the DRE for any election. We have also recommended that SBE enhance the controls for certifying that the implemented source code is the same version as that certified by the ITA and to expand their testing to include testing for time-oriented exploits (e.g., trojans). This may be accomplished by changing the machine date and time to correspond to that of the election during testing.
4	*"We also note that the software is written entirely in C++. When programming in an unsafe language like C++, programmers must exercise tight discipline to prevent their programs from being vulnerable to buffer overflow attacks and other weaknesses."*	M-1, M-5, O-34	The scope of the risk assessment did not include a review of Diebold's software engineering practices or an evaluation of which software language may be more secure. Our review did note vulnerabilities that point to software inconsistencies and problems. SBE and LBE's Logic & Accuracy tests verify that votes are recorded accurately prior to the use of the DRE for any election. We have also recommended that SBE enhance the controls for certifying that the implemented source code is the same version as that certified by the ITA and to expand their testing to include testing for time-oriented exploits (e.g., trojans). This may be accomplished by changing the machine date and time to correspond to that of the election during testing.
4	*"Indeed, buffer overflows caused real problems for AccuVote-TS systems in real elections."* (Note: This reference has nothing to do with buffer overflows)	N/A	It is true that this system is not configured to defend against buffer overflow attacks. As the DRE has no network connections, an attacker is not provided a means to exploit this vulnerability.
4	*"Although the Diebold code is designed to run on a DRE device (an example of which is shown in Figure 1), one can run it on a regular Microsoft Windows computer (during our experiments we compiled and ran the code on a Windows 2000 PC)."*	N/A	This is not a security requirement.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
4	*"In the following we describe the process for setting up and running an election using the Diebold system. Although we know exactly how the code works from our analysis, we must still make some assumptions about the external processes at election sites. In all such cases, our assumptions are based on the way the Diebold code works, and we believe that our assumptions are reasonable. There may, however, be additional administrative procedures in place that are not indicated by the source code."*	N/A	This is not a security requirement, but it does give insight into the methodology used by the Rubin team in the drafting the report.
5	*"In common usage, we believe the voting terminals will be distributed without a ballot definition pre-installed."*	M-7, M-10, O-8	This assumption is invalid. The voting terminals are distributed with the state approved ballot information loaded.
5	*"We do not know exactly how the voter gets his voter card. It could be sent in the mail with information about where to vote, or it could be given out at the voting site on the day of the election. To understand the voting software itself, however, we do not need to know what process is used to distribute the cards to voters."*	O-103	This assumption is invalid. The Voter Access Cards are distributed at the polling site after the voter is vetted, and retrieved from the voter after the voter has cast their vote.
5	*"As we have only analyzed the code for the Diebold voting terminal, we do not know exactly how the back-end server tabulates the final results it gathers from the individual terminals. Obviously, it collects all the votes from the various voting terminals. We are unable to verify that there are checks to ensure, for example, that there are no more votes collected than people who are registered at or have entered any given polling location."*	M-1, M-5, O-16, O-91	SBE and LBEs have numerous checks and balances to ensure that the votes entered on the DRE devices are accurately reported. There are checks at the polling site, the LBE HQ and SBE. SAIC has recommended that the checks and balances be augmented to include a 100% verification of the vote transmissions to the PCMCIA cards.
9	*"Upon reviewing the Diebold code, we observed that the smartcards do not perform any cryptographic operations."*	NA	That is correct, the smartcards perform no cryptographic functions. The smartcards also do not contain any sensitive or personal information. The smartcards contain party affiliation (in the case of a primary election) and access to vote on the DRE.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
9	*"For example, authentication of the terminal to the smartcard is done "the old-fashioned way:" the terminal sends a clear text (i.e., unencrypted) 8-byte password to the card and, if the password is correct, the card believes that it is talking to a legitimate voting terminal. Unfortunately, this method of authentication is insecure: an attacker can easily learn the 8-byte password used to authenticate the terminal to the card (see Section 3.3), and thereby communicate with a legitimate smartcard using his own smartcard reader."*	M-5, M-83, M-124, O-12, O-15, O-36, O-92,	The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to attach a card reader to the voting terminal would be easily visible to any of the many election officials. In addition, the vetting process limits access to DRE devices to eligible voters.
9	*"Furthermore, there is no authentication of the smartcard to the device. This means that nothing prevents an attacker from using his own homebrew smartcard in a voting terminal."*	M-5, M-83, O-12, O-15, O-36, O-92	Although it is possible for someone to buy and to program their own smartcard, the attacker would be limited to changing their party affiliation in the case of a primary (i.e., they could see a ballot meant for another party) because the smartcard only contains party affiliation and access to vote on the DRE. The combination of logic controls in the DRE software, the physical controls and the openness of the voting booths minimize the likelihood of the voter being able to cast multiple votes without being detected.
9	*"An attacker who knows the protocol spoken by the voting terminal to the legitimate smartcard could easily implement a homebrew card that speaks the same protocol."*	M-5, M-83, O-12, O-15, O-36, O-91, O-92,	Although it is possible for someone to buy and to program their own smartcard, the attacker would be limited to changing their party affiliation in the case of a primary (i.e., they could see a ballot meant for another party) because the smartcard only contains party affiliation and access to vote on the DRE. The combination of logic controls in the DRE software, the physical controls and the openness of the voting booths minimize the likelihood of the voter being able to cast multiple votes without being detected.
9	*"Even if the attacker does not a priori know the protocol, an attacker could easily learn enough about the protocol to create new voter cards by attaching a "wiretap" device between the voting terminal and a legitimate smartcard and observing the communicated messages."*	M-5, M-83, O-12, O-15, O-36, O-92	The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to attach a card reader to the voting terminal would be easily visible to any of the many election officials. In addition, the vetting process limits access to DRE devices to eligible voters.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
			limits access to DRE devices to eligible voters.
9	*"The parts for building such a device are readily available and, given the privacy of voting booths, might be unlikely to be noticed by poll workers. An attacker might not even need to use a wiretap to see the protocol in use."*	M-5, O-12, O-36	The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to attach a card reader to the voting terminal would be easily visible to any of the many election officials.
9	*"Likewise, the important data on the legitimate voting card is stored as a file (named 0x3D40 — smartcard files have numbers instead of textual file name) that can be easily read by a portable smartcard reader. Again, given the privacy of voting booths, an attacker using such a card reader would be unlikely to be noticed. Given the ease with which an attacker can interact with legitimate smartcards, plus the weak password-based authentication scheme (see Section 3.3), an attacker could quickly gain enough insight to create homebrew voting cards, perhaps quickly enough to be able to use such homebrew cards during the same election day."*	M-5, O-91	The privacy of the voting booth is limited. If one pictures the old, curtained voting booths of the past, this could be possible. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to attach a card reader to the voting terminal would be easily visible to any of the many election officials.
9	*"The only impediment to the mass production of homebrew smartcards is that each voting terminal will make sure that the smartcard has encoded in it the correct m_ElectionKey, m_VCenter, and m_DLVersion (see DoVote() in BallotStation/Vote.cpp). The m_ElectionKey and m_DLVersion are likely the same for all locations and, furthermore, for backward-compatibility purposes it is possible to use a card with m_ElectionKey and m_DLVersion undefined. The m_VCenter value could be learned on a per-location-basis by interacting with legitimate smartcards, from an insider, or from inferences based on the m_VCenter values observed at other polling locations."*	M-16, M-17, M-32, O-4, O-12, O-14	Although it is possible for someone to buy and to program their own smartcard, the attacker would be limited to changing their party affiliation in the case of a primary (i.e., they could see a ballot meant for another party) because the smartcard only contains party affiliation and access to vote on the DRE. The combination of logic controls in the DRE software, the physical controls and the openness of the voting booths minimize the likelihood of the voter being able to cast multiple votes without being detected.
10	*"Since an adversary can make perfectly valid smartcards, the adversary could bring a stack of active cards to the*	M-83, 112, M-113, O-	The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	voting booth. Doing so gives the adversary the ability to vote multiple times."	91	the voter's selections. The action of trying to run numerous smartcards through the voting terminal would be easily visible to any of the many election officials. In addition, the voting machine makes a loud noise and ejects the smartcard after each vote is cast.
10	*"More simply, instead of bringing multiple cards to the voting booth, the adversary could program a smartcard to ignore the voting terminal's deactivation command. Such an adversary could use one card to vote multiple times."*	M-83, M-88, M-113, O-91	The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to cast multiple votes would be easily visible to any of the many election officials. Additionally, there are procedures to ensure that only the correct number of votes have been cast on each DRE. Each polling site checks the number of Voter Authority Cards signed, to the register, then to the total votes cast on DREs.
10	*"Will the adversary's multiple-votes be detected by the voting system? To answer this question, we must first consider what information is encoded on the voter cards on a per-voter basis. The only per-voter information is a "voter serial number" (m_VoterSN in the CVoterInfo class). Because of the way the Diebold system works, m_VoterSN is only recorded by the voting terminal if the voter decides not to place a vote (as noted in the comments in TSElection/Results.cpp, this field is recorded for uncounted votes for backward compatibility reasons). It is important to note that if a voter decides to cancel his or her vote, the voter will have the opportunity to vote again using that same card (and, after the vote has been cast, m_VoterSN will not be recorded)."*	M-9, M-132, M-136, M-142	There are procedures to ensure that only the correct number of votes have been cast on each DRE. Each polling site checks the number of Voter Authority Cards signed, to the register, then to the total votes cast on DREs.
10	*"Can the back-end tabulation system detect multiple-vote casting? If we assume the number of collected votes becomes greater than the number of people who showed up to vote, and if the polling locations keep accurate counts of the number of people who show up to vote, then the back-end system, if designed properly, should be able*	M-9, M-132, M-136, M-142, O-91	As noted, Mr. Rubin did not look at the backend tabulating system. SBE and LBE have numerous checks and balances to ensure that the votes entered on the DRE devices are accurately reported. There are checks at the polling site, the LBE HQ and SBE. SAIC has recommended that the checks and balances be augmented to include a

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	to detect the existence of counterfeit votes. However, because m_VoterSN is only stored for those who did not vote, there will be no way for the tabulating system to count the true number of voters or distinguish the real votes from the counterfeit votes. This would cast serious doubt on the validity of the election results. We point out, however, that we only analyzed the voting terminal's code; we do not know whether such checks are performed in the actual back-end tabulating system."		100% verification of the vote transmissions to the PCMCIA cards.
10	*"Just as an adversary can manufacture his or her own voter cards, an adversary can manufacture his or her own administrator and ender cards (administrator cards have an easily-circumventable PIN, which we will discuss in Section 3.2). This attack is easiest if the attacker has knowledge of the Diebold code or can interact with a legitimate administrator or ender card."*	M-83, O-4, O-12	Assuming someone could manufacture the card and obtained access to the DRE, the specific DRE device could be disabled (i.e., close election). Such an attack would be detected due to the physical controls and the openness of the voting booths. The Disaster Recovery and Incident Management Plan guide provides procedures for handling a disabled DRE.
10	*"Using a homebrew administrator card, a poll worker, who might not otherwise have access to the administrator functions of the Diebold system but who does have access to the voting machines before and after the elections, could gain access to the administrator controls. If a malicious voter entered an administrator or ender card into the voting device instead of the normal voter card, then the voter would be 10 able to terminate the election and, if the card is an administrator card, gain access to additional administrative controls."*	M-1, M-13, O-4, O-12, O-14, O-17	Assuming someone could manufacture the card and obtained access to the DRE, the specific DRE device could be disabled (i.e., close election). Such an attack would be detected due to the physical controls and the openness of the voting booths. The Disaster Recovery and Incident Management Plan guide provides procedures for handling a disabled DRE.
11	*"The use of administrator or ender cards prior to the completion of the actual election represents an interesting*	M-1, M-5, M-83, M[illegible]	Assuming someone could manufacture the card and obtained access to the DRE, the specific DRE device could

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	completion of the actual election represents an interesting denial-of-service attack. Once "ended," the voting terminal will no longer accept new voters (see CVoteDlg::OnCardIn()) until the terminal is somehow reset. Such an attack, if mounted simultaneously by multiple people, could shut down a polling place. If a polling place is in a precinct considered to favor one candidate over another, attacking that specific polling place could benefit the less-favored candidate. Even if the poll workers were later able to resurrect the systems, the attack might succeed in deterring a large number of potential voters from voting (e.g., if the attack was performed over the lunch hour). If such an attack was mounted, one might think the attackers would be identified and caught. We note that many governmental entities do not require identification to be presented by a voter, instead allowing for "provisional" ballots to be cast. By the time the poll workers realize that one of their voting terminals has been disabled, the perpetrator may have long-since left the scene."	M-83, M-88, M-91, M-113, O-4, O-14, O-22	obtained access to the DRE, the specific DRE device could be disabled (i.e., close election). Such an attack would be detected due to the physical controls and the openness of the voting booths. The Disaster Recovery and Incident Management Plan guide provides procedures for handling a disabled DRE. If as suggested, multiple individuals mounted a simultaneous attack at a polling site, with forged administrator cards, and closed the DRE devices, and we assume that they all successfully got away, the Election Judges still could immediately reopen the DRE devices. The Disaster Recovery and Incident Management Plan guide provides procedures for handling a disabled DRE.
11	*"Upon looking more closely at this administrator authentication process, however, we see that there is a flaw with the way the PINs are verified. When the terminal and the smartcard first begin communicating, the PIN value stored on the card is sent in cleartext from the card to the voting terminal. Then, when the user enters the PIN into the terminal, it is compared with the PIN that the smartcard sent (CPinDlg::OnOK()). If these values are equal, the system accepts the PIN. Herein lies the flaw with this design: any person with a smartcard reader can easily extract the PIN from an administrator card. The adversary doesn't even need to fully understand the protocol between the terminal and the device: if the response from the card is n bytes long, the attacker who correctly guesses that the PIN is sent in the clear would only have to try n¡3 possible PINs, rather than 10,000. This*	M-1, M-5, O-4, O-14	Assuming someone could manufacture the card and obtained access to the DRE or obtained a valid administrator's card and PIN combinations, the specific DRE device could be disabled (i.e., close election). Such an attack would be detected due to the physical controls and the openness of the voting booths. The Disaster Recovery and Incident Management Plan guide provides procedures for handling a disabled DRE. Additionally the privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	means that the PINs are easily circumventable. Of course, if the adversary knows the protocol between the card and the device, an adversary could just make his own administrator card, using any desired PIN (Section 3.1.2)."		
12	*"There are several issues with the above code. First, hard-coding passwords in C++ files is generally a poor design choice. We will discuss coding practices in more detail in Section 6, but we summarize some issues here. Hard-coding passwords into C++ files suggests a lack of key and password management."*	M-111	Hard-coding of passwords is not consistent with best security practice. We have recommended that the hard-coded passwords be removed and changed.
12	*"Furthermore, even if the developers assumed that the passwords would be manually changed and the software recompiled on a per-election basis, it would be very easy for someone to forget to change the constants in VoterCard/CLXSmartCard.cpp. (Recompiling on a per-election basis may also be a concern, since good software engineering practices would dictate additional testing and certification if the code were to be recompiled for each election.)"*	M-1, M-5, M-111	This assumption is invalid assumption. The software is not recompiled on a per-election basis. In addition, only source code certified by the ITA is loaded on the devices. SBE and LBE's Logic & Accuracy tests verify that votes are recorded accurately. SAIC has recommended that SBE enhance the controls for certifying that the implemented source code is the same verison as that certified by the ITA and to expand their testing to include testing for time-oriented exploits (e.g., trojans). This may be accomplished by changing the machine date and time to correspond to that of the election during testing.
12	*"The above issues would only be a concern if the authentication method were otherwise secure. Unfortunately, it is not. Since the password is sent in the clear from the terminal to the card, an attacker who puts a fake card into the terminal and records the command from the terminal will be able to learn the password (and file name) and then re-use that password with real cards. An adversary with knowledge of this password could then create counterfeit voting cards. As we have already discussed (see Section 3.1.1), this can allow the adversary to cast multiple votes, among other attacks. Hence, the authentication of the voting terminal to the smartcards is*	M-1, M-5, M-95, M-111, M-112, O-12, O-35	The smartcard allows the voter to enter a vote, but the user is authenticated during the vetting process, (i.e., the control over who gets to vote is not controlled by the smartcard, but by the vetting procedures). Once again the privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to cast multiple votes would be easily visible to any of the many election officials. In addition, the voting machine makes a loud noise and ejects the smartcard after each vote is cast.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	insecure."		
12	*"Furthermore, note the control flow in the above code-snippet. If the password chosen by the designers of the system ("\xED\x0A\xED\x0A\xED\x0A\xED\x0A") does not work, then CCLXSmartCard::* *Open() uses the smartcard manufacturer's default password of "\x00\x01\x02\x03\x04\x05\x06\x07."* *One issue with this is that it implies that sometimes the system is used with un-initialized smartcards. This means that an attacker might not even need to figure out the system's password in order to be able to authenticate to the cards."*	M-83, M-86	The smartcard allows the voter to enter vote, but the user is authenticated during the vetting process, (i.e., the control over who gets to vote is not controlled by the smartcard, but by the vetting procedures). In addition, once again the privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to cast multiple votes would be easily visible to any of the many election officials. In addition, the voting machine makes a loud noise and ejects the smartcard after each vote is cast.
12	*"As we noted in Section 3.1, some smartcards allow a user to get a listing of all the files on a card. If the system uses such a card and also uses the manufacturer's default password of \x00\x01\x02\x03\x04\x05\x06\x07, then an attacker, even without any knowledge of the source code and without the ability to intercept the connection between a legitimate card and a voting terminal, but with access to a legitimate voter card, will still be able to learn enough about the smartcards to be able to create counterfeit voter cards."*	M-83, M-88	The smartcard allows the voter to enter vote, but the user is authenticated during the vetting process, (i.e., the control over who gets to vote is not controlled by the smartcard, but by the vetting procedures). Once again the privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to cast multiple votes would be easily visible to any of the many election officials. In addition, the voting machine makes a loud noise and ejects the smartcard after each vote is cast.
13	*"Unfortunately, under Windows CE, which we believe is used in commercial Diebold voting terminals, the existence of the removable storage device is not enforced properly."*	M-5	The PCMCIA cards are locked into the DRE device. The key is controlled by the Chief Judges. Additionally, we have recommended that the State further secure this locked compartment using tamper-proof tape during the actual election
13	*"Unlike other versions of Windows, removable storage cards are mounted as subdirectories under CE. When the voting software wants to know if a storage card is inserted, it simply checks to see if the Storage Card subdirectory*	M-83, M-112, M-113	Pre-election Logic and Accuracy testing checks both the main storage area, and the removable memory.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	exists in the filesystem's root directory. While this is the default name for a mounted storage device, it is also a perfectly legitimate directory name for a directory in the main storage area. Thus, if such a directory exists, the terminal can be fooled into using the same storage device for all of the data. This would reduce the amount of redundancy in the voting system and would increase the chances that a hardware fault could cause recorded votes to be lost."		
13	*"The majority of the system configuration information for each terminal is stored in the Windows registry under HKEY_LOCAL_MACHINE\Software\GlobalElectionSystems\AccuVote-TS4 . This includes both identification information such as the terminal's serial number and more traditional configuration information such as the COM port that the smartcard reader is attached to. All of the configuration information is stored in the clear, without any form of integrity protection. Thus, all an adversary must do is modify the system registry to trick a given voting terminal into effectively impersonating any other voting terminal."*	M-83, M-112, M-113, M-120, O-12, O-17, O-35	Exploitation of this vulnerability requires access to the system registry. Since the DRE is not connected to a network, an attacker's access to the registry is limited by procedural and physical barriers.
13	*"It is unclear how the tallying authority would deal with results from two different voting terminals with the same voting ID — at the very least human intervention to resolve the conflict would probably be required."*	M-1, M-5	Prior to each election, the GEMS server assigns a unique number to each PCMCIA card as part of the ballot loading process. When the results are read from the PCMCIA cards at the conclusion of the election, the GEMS server uses this unique number to validate acceptance of the data. If two of these numbers are identical, the election officials would investigate using established procedures.
13	*"The Federal Election Commission draft standard requires each terminal to keep track of the total number of votes that have ever been cast on it — the "Protective Counter." This counter is used to provide yet another method for ensuring that the number of votes cast on each terminal is correct. However, as the following code from*	M-121, M-167, O-7, O-96, T-11	This exploit requires access to the system. Since the system is not connected to a network, physical access is required. The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to connect devices to the system would be easily visible to any

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	Utilities/machine.cpp shows, the counter is simply stored as an integer in the file system.bin in the terminal's system directory (error handling code has been removed for clarity): *long GetProtectedCounter()* *{* *DWORD protectedCounter = 0;* *CString filename = ::GetSysDir();* *filename += _T("system.bin");* *CFile file;* *file.Open(filename, CFile::modeRead | CFile::modeCreate |* *CFile::modeNoTruncate);* *file.Read(&protectedCounter, sizeof(protectedCounter));* *file.Close();* *return protectedCounter;* *}* *By modifying this counter, an adversary could cast doubt on an election by creating a discrepancy between the number of votes cast on a given terminal and the number of votes that are tallied in the election. While the current method of implementing the counter is totally insecure, even a cryptographic checksum would not be enough to*		of the many election officials. Other physical and procedural controls are effective in preventing access to the system prior to, or after an election.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	protect the counter; an adversary with the ability to modify and view the counter would still be able to roll it back to a previous state. In fact, the only solution that would work would be to implement the protective counter in a tamper-resistant hardware token, requiring modifications to the physical voting terminal hardware."		
14	*"The "ballot definition" for each election contains everything from the background color of the screen to the PPP username and password to use when reporting the results. This data is not encrypted or check summed (cryptographically or otherwise) and so can be easily modified by any attacker with physical access to the file."*	M-7, M-8, M-10, O-14	As stated, this assumption requires access to the system. Since the system is not connected to a network, physical access is required. The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to connect devices to the DRE would be easily visible to any of the many election officials.
14	*"By simply changing the order of the candidates as they appear in the ballot definition, the results file will change accordingly. However, the candidate information itself is not stored in the results file. The file merely tracks that candidate 1 got so many votes and candidate 2 got so many other votes. If an attacker reordered the candidates on the ballot definition, voters would unwittingly cast their ballots for the wrong candidate. As with denial-of-service attacks (see Section 3.1.2), ballot reordering attacks would be particularly effective in polling locations known to be heavily partisan."*	M-7, M-8, O-3, O-14	This exploit requires access to the system. Since the system is not connected to a network, physical access is required. The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to connect devices to the system would be easily visible to any of the many election officials. In addition, the ballot is on the PCMCIA card, which is locked in the DRE device. Note: SBE uses a public FTE site to distribute ballot information. While there are many checks at the LBE of the ballot, SAIC has recommended that SBE implement a secure method to transfer the ballot.
14	*"Even without modifying the ballot definition, an attacker can gain almost enough information to impersonate the voting terminal to the back-end server. The terminal's voting center ID, PPP dial-in number, username, password and the IP address of the back-end server are all available in the clear (these are parsed into a CElectionHeaderItem in TSElection\TSElectionObj.cpp). Assuming an attacker is able to guess or create a voting terminal ID, he would be*	M-5; M-14, M-39, O-23	The LBE GEMS server (i.e., backend server) is not connected to a network. The LBE GEMS server checks for PCMCIA cards from the modem transmissions. This error checking accounts both for card validity (i.e. that the card was issued and is not a duplicate) and ensures that all issued cards are reported. SAIC has recommended that the modem transmissions be

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	able to transmit fraudulent vote reports to the backend server by dialing in from his own computer. While both the paper trail and data stored on legitimate terminals could be used to compensate for this attack after the fact, it could, at the very least, delay the election results."		encrypted and that the LBE perform a 100% verification of the vote transmissions to PCMCIA cards.
14	*"(The PPP number, username, password, and IP address of the back-end server are also stored in the registry HKEY_LOCAL_MACHINE\Software\GlobalElectionSystems\AccuVote-TS4\ TransferParams. Since the ballot definition may be transported on portable memory cards or floppy disks, the ballot definition may perhaps be easier to obtain from this distribution media rather than from the voting terminal's internal data storage.)"*	M-83, M-89, M-91	Ballots are public knowledge. After the ballot is created at SBE, the LBE performs the Logic and Accuracy tests to ensure validity and correctness.
14	*"We will return to some of these points in Section 5.1, where we show that modifying and viewing ballot definition files does not always require physical access to the terminals on which they are stored."*	M-83, M-91	Modification of the ballot requires access to the PCMCIA cards since the DRE devices are not connected to a network.
15	*"Unlike the other data stored on the voting terminal, both the vote records and the audit logs are encrypted and check summed before being written to the storage device. Unfortunately, neither the encrypting nor the check summing is done securely.* *All of the data on a storage device is encrypted using a single, hard-coded DES [NBS77] key:* *#define DESKEY ((des_key*)"F2654hD4")"*	M-41, M-124	Currently, ~~DES~~ encryption is only used for the resident DRE memory. Once the DRE is powered down, the memory is erased. Note, we have recommended that encryption be employed for the modem transmission of the vote totals. The DRE devices are not connected to a network and physical access would be required to get to the data. The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to connect devices to the system would be easily visible to any of the many election officials.
15	*"Note that this value is not a hex representation of a key. Instead, the bytes in the string "F2654hD4" are fed directly into the DES key scheduler. If the same binary is used on every voting terminal, an attacker with access to the*	M-1, M-5, M-111	Currently, ~~DES~~ encryption is only used for the resident DRE memory. Once the DRE is powered down, the memory is erased. Note, we have recommended that encryption be employed for the modem transmission of the vote totals.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	source code, or even to a single binary image, could learn the key, and thus read and modify voting and auditing records."		employed for the modem transmission of the vote totals. The DRE devices are not connected to a network and physical access would be required to get to the data. The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to connect devices to the system would be easily visible to any of the many election officials.
15	*"Even if proper key management were to be implemented, many problems would still remain. First, DES keys can be recovered by brute force in a very short time period [Gil98]. DES should be replaced with either triple-DES [Sch96] or, preferably, AES [DJ02]."*	M-41, M-124	We found no evidence that data was encrypted. However, the devices are not connected to a network and physical access would be required to get to the data. The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to connect devices to the system would be easily visible to any of the many election officials.
15	*"Second, DES is being used in CBC mode which requires an initialization vector to ensure its security. The implementation here always uses zero for its IV. This is illustrated by the call to DesCBCEncrypt in TSElection/RecordFile.cpp;* *since the second to last argument is NULL, DesCBCEncrypt will use the all-zero IV.* *DesCBCEncrypt((des_c_block*)tmp, (des_c_block*)record.m_Data, totalSize,* *DESKEY, NULL, DES_ENCRYPT);* *This allows an attacker to mount a variety of cryptanalytic attacks on the data."*	M-41, M-124,	Currently, ~~DES~~ encryption is only used for the resident DRE memory. Once the DRE is powered down, the memory is erased. Note, we have recommended that encryption be employed for the modem transmission of the vote totals. The DRE devices are not connected to a network and physical access would be required to get to the data. The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to connect devices to the system would be easily visible to any of the many election officials.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
15	*"Before being encrypted, a 16-bit cyclic redundancy check (CRC) of the plaintext data is computed. This CRC is then stored along with the ciphertext in the file and verified whenever the data is decrypted and read. This process in handled by the ReadRecord and WriteRecord functions in TSElection/ RecordFile.cpp. Since the CRC is an unkeyed, public function, it does not provide any real integrity for the data. In fact, by storing it in an unencrypted form, the purpose of encrypting the data in the first place (leaking no information about the contents of the plaintext) is undermined. A much more secure design would be to first encrypt the data to be stored and then to compute a keyed cryptographic checksum (such as HMAC-SHA1 [BCK96]) of the ciphertext. This cryptographic checksum could then be used to detect any tampering with the plaintexts. Note also that each entry has a timestamp, which will prevent the re-ordering, though not deletion, of records. Each entry in a plaintext audit log is simply a time stamped, informational text string. At the time that the logging occurs, the log can also be printed to an attached printer. If the printer is unplugged, off, or malfunctioning, however, no record will be stored elsewhere to indicate that the failure occurred. The following code from TSElection/Audit.cpp demonstrates that the designers failed to consider these issues:* *if (m_Print && print) {* *CPrinter printer;* *// If failed to open printer then just return.* *CString name = ::GetPrinterPort();* *if (name.Find(_T("\\")) != -1)*	M-41, M-124	Currently, ~~DES~~ encryption is only used for the resident DRE memory. Once the DRE is powered down, the memory is erased. Note, we have recommended that encryption be employed for the modem transmission of the vote totals. The DRE devices are not connected to a network and physical access would be required to get to the data. The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to connect devices to the system would be easily visible to any of the many election officials.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	name = GetParentDir(name) + _T("audit.log"); *if (!printer.Open(name, ::GetPrintReverse(), FALSE))* *::TSMessageBox(_T("Failed to open printer for logging"));* *} else {* *15* *Do the printing: : :}* *If the cable attaching the printer to the terminal is exposed, an attacker could create discrepancies between the printed log and the log stored on the terminal by unplugging the printer (or, by simply cutting the cable)."*		
16	*"An attacker's most likely target will be the voting records, themselves. Each voter's votes are stored as a bit array based on the ordering in the ballot definition file along with other information such as the precinct the voter was in, although no information that can be linked to a voter's identity is included. If the voter has chosen a write-in candidate, this information is also included as an ASCII string. An attacker given access to this file would be able to generate as many fake votes as he or she pleased, and such votes would be indistinguishable from the true votes cast on the terminal."*	M-1, M-5, M-14, O-12, O-14	The devices are not connected to a network and physical access would be required to get to the data. The privacy of the voting booth is limited. The AccuVote voting booth provides privacy only for the touch screen and the voter's selections. The action of trying to connect devices to the system would be easily visible to any of the many election officials. Additionally, in the State of Maryland implementation, the total votes recorded on the DRE is reconciled with the number of votes cast on the DRE using the paper Voter Authority Card that is placed into the Voter Authority Card envelope, attached to the DRE voting terminal by the election official.
16	*"While the voter's identity is not stored with the votes, each vote is given a serial number. These serial numbers are generated by a linear congruential random number generator (LCG), seeded with static information about the election and voting terminal. No dynamic information, such as the current time, is used.*	T-43	The anonymity of a voter's ballot is preserved because the AccuVote-TS voting system does not use or store personal information and does not provide an individual paper record for each voter, therefore leaving no evidence of a single voter's selections. The individual ballots however, are stored sequentially. If someone kept track of all of the individuals who voted on a particular DRE and then was able to obtain

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	// LCG - Linear Conguential Generator - used to generate ballot serial numbers *// A psuedo-random-sequence generator* *// (per Applied Cryptography, by Bruce Schneier, Wiley, 1996)* *#define LCG_MULTIPLIER 1366* *#define LCG_INCREMENTOR 150889* *#define LCG_PERIOD 714025* *static inline int lcgGenerator(int lastSN)* *{* *return ::mod(((lastSN * LCG_MULTIPLIER) + LCG_INCREMENTOR), LCG_PERIOD);* *}* *While the code's authors apparently decided to use an LCG because it appeared in Applied Cryptography[Sch96], LCG's are far from secure. However, attacking this random number generator is unnecessary for determining the order in which votes were cast: each vote is written to the file sequentially. Thus, if an attacker is able to determine the order in which voters cast their ballots, the results file has a nice list, in the order in which voters used the terminal. A malevolent poll worker, for example, could surreptitiously track the order in which voters use the voting terminals. Later, in collaboration with other attackers who might intercept the poorly encrypted voting records, the exact voting record of each voter could be*		who voted on a particular DRE and then was able to obtain the PCMCIA card, they would be able to tie votes back to individuals. However this would require collusion between multiple individuals.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	reconstructed."		
16	*"Physical access to the voting results may not even be necessary to acquire the voting records, if they are transmitted across the Internet."*	O-23, 0-24	Voting records are not transmitted via the Internet in the State of Maryland implementation.
17	*"We first note that it is possible for an adversary to tamper with the voting terminals' ballot definition file (election.edb). If the voting terminals load the ballot definition from a floppy or removable storage card, then an adversary, such as a poll worker, could tamper with the contents of the floppy before inserting it into the voting terminal."*	M-7, M-89, O-7, O-14	LBEs do load ballots and a malicious worker could tamper with this process. Each LBE has policies and procedures in place, such as a two-person rule, to limit any single individuals access to voting terminals. The Logic and Accuracy testing preformed prior to the election, would uncover any falsified ballots.
17	*"On a potentially much larger scale, if the voting terminals download the ballot definition from the Internet, then an adversary could tamper with the ballot definition file en-route from the back-end server to the voting terminal. With respect to the latter, we point out that the adversary need not be an election insider; the adversary could, for example, be someone working at the local ISP."*	M-7, M-8, O-23	DRE devices are distributed with the approved ballots loaded and locked into the machine. The machines are sealed with tamper-proof tape prior to shipment to the polling site. The Election Judges remove the tamper-proof tape the morning of the election.
17	*"If a wireless network is used, anybody within radio range becomes a potential adversary. With high-gain antennas, the adversary can be sufficiently distant to have little risk of detection. If the adversary knows the structure of the ballot definition, then the adversary can intercept and modify the ballot definition while it is being transmitted. Even if the adversary does not know the precise structure of the ballot definition, many of the fields inside are easy to identify and change, including the candidates' names, which appear as plain ASCII text.10"*	O-23, O-24	Wireless networking is not used.
17	*"Let us now consider some example attacks that make use of modifying the ballot definition file. Because no cryptographic techniques are in place to guard the integrity of the ballot definition file, an attacker could add, remove, or change issues on the ballot, and thereby confuse the*	M-7, M-41, M-124, O-14, T-37	DRE devices are distributed with the approved ballots loaded and locked into the machine. The machines are sealed with tamper-proof tape prior to shipment to the polling site. The Election Judges remove the tamper-proof tape the morning of the election.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	result of the election."		tape the morning of the election.
17	*"Likewise, an attacker who can change the ballot definition could also change the ordering of the candidates running for a particular office. Since, at the end of the election, the results are uploaded to the server in the order that they appear in the ballot definition file, and since the server will believe that the results appear in their original order, this attack could also succeed in swapping the votes between parties in a predominantly partisan precinct. This ballot reordering attack is also discussed in more detail in Section 4.3."*	M-7, M-10	DRE devices are distributed with the approved ballots loaded and locked into the machine. The machines are sealed with tamper-proof tape prior to shipment to the polling site. The Election Judges remove the tamper-proof tape the morning of the election.
17	*"Suppose that the election officials are planning to download the configuration files over the Internet and that they are running late and do not have much time before the election starts to distribute ballot definitions manually (i.e., they might not have enough time to distribute physical media with the ballot definition files from central office to every voting precinct). In such a situation, an adversary could mount a traditional Internet denial-of-service attack against the election management's server and thereby prevent the voting terminals from acquiring their ballot definitions before the start of the election. To mount such an attack effectively, the adversary would ideally need to know the topology of the system's network, and the name of the server(s) supplying the ballot definition file.12 If a fair number of people from a certain demographic plan to vote early in the morning, then this could impact the results of the election."*	N/A	DRE devices are distributed with the approved ballots loaded and locked into the machine. The machines are sealed with tamper-proof tape prior to shipment to the polling site. The Election Judges remove the tamper-proof tape the morning of the election.
18	*"Unlike such traditional attacks, however, the network-based attack (1) is relatively easy for anyone with knowledge of the election system's network topology to accomplish; (2) this attack can be performed on a very large scale, as the central distribution point(s) for ballot definitions becomes an effective single point of failure; and*	O-23, O-24	The DRE devices are not connected to the Internet or to any other network. The DRE devices are distributed with the approved ballots loaded and locked into the machine. The machines are sealed with tamper-proof tape prior to shipment to the polling site. The Election Judges remove the tamper-proof tape the morning of the election.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	(3) the attacker can be physically located anywhere in the Internet-connected world, complicating efforts to apprehend the attacker. Such attacks could prevent or delay the start of an election at all voting locations in a state. We note that this attack is not restricted to the system we analyzed; it is applicable to any system that downloads its ballot definition files using the Internet."		tamper-proof tape the morning of the election.
18	*"Just as it is possible for an adversary to tamper with the downloading of the ballot definition file (Section 5.1), it is also possible for an adversary to tamper with the uploading of the election results. To make this task even easier for the adversary, we note that although the election results are stored "encrypted" on the voting devices (Section 4.4), the results are sent from the voting devices to the back-end server over an unauthenticated and unencrypted channel. In particular, CTransferResultsDlg::OnTransfer() writes ballot results to an instance of CDL2Archive, which then writes the votes in cleartext to a socket without any cryptographic checksum. Sending election results in this way over the Internet is a bad idea. Nothing prevents an attacker with access to the network traffic, such as workers at a local ISP, from modifying the data in transit."*	M-89, O-23	The Internet is not used for transmitting voting counts.
18	*"If the voting terminals use a modem connection directly to the tabulating authority's network, rather than the Internet, then the risk of such an attack is less, although still not inconsequential. A sophisticated adversary (or employee of the local phone company) could tap the phone line and intercept the communication."*	O-23, O-24	Modem communications are subject to intercept. SAIC has recommended: a) encryption for the transmissions; b) a 100% verification of PCMCIA cards to the vote transmissions.
18	*"All of these adversaries could be easily defeated by properly using standard encryption suites like SSL/TLS, used throughout the World Wide Web for e-commerce security. We are puzzled why such a widely accepted and studied technology is not used by the voting terminals to*	O-23, O-24	Modem communications are subject to intercept. SAIC has recommended: a) encryption for the transmissions; b) a 100% verification of PCMCIA cards to transmissions.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	safely communicate across potentially hostile networks."		
18	*"In some configurations, where the voting terminals are directly connected to the Internet, it may be possible for an adversary to attack them directly, perhaps using an operating system exploit or buffer overflow attack of some kind. Ideally the voting devices and their associated firewalls would be configured to accept no incoming connections [CBR03]. This concern would apply to any voting terminal, from any vendor, with a direct Internet connection."*	O-23, O-24	The DRE device is not connected to the Internet or to any other network.
19	*"Of course, reading the source code to a product gives only an incomplete view into the actions and intentions of the developers who created that code. Regardless, we can see the overall software design, we can read the comments in the code, and thanks to the CVS repository, we can even look at earlier versions of the code and read the developers' commentary as they committed their changes to the archive."*	N/A	This is not a security requirement.
19	*"Inside cvs.tar we found multiple CVS archives. Two of the archives, AccuTouch and AVTSCE implement full voting terminals. The AccuTouch code dates to around 2000 and is copyrighted by "Global Election Systems, Inc." while the AVTSCE code dates to mid-2002 and is copyrighted by "Diebold Election Systems, Inc." (The CVS logs show that the copyright notice was updated on February 26, 2002.) Many files are nearly identical between the two systems and the overall design appears very similar. Indeed, Diebold acquired Global Election Systems in September, 2001.13 Some of the code, such as the functions to compute CRCs and DES, dates back to 1996, when Global Election Systems was called "I-Mark Systems."* *This legacy is apparent in the code itself as there are portions of the AVTSCE code, including entire classes,*	N/A	This is not a security requirement.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	that are either simply not used or removed through the use of #ifdef statements. Many of these functions are either incomplete or, worse, do not perform the function that they imply as is the case with *CompareFiles in Utilities/FileUtil.cpp:* *BOOL CompareFiles(const CString& file1, const CString& file2)* *{* */* XXX use a CRC or something similar */* *BOOL exists1, exists2;* *HANDLE hFind;* *WIN32_FIND_DATA fd1, fd2;* *exists1 = ((hFind = ::FindFirstFile(file1, &fd1)) != INVALID_HANDLE_VALUE);* *::FindClose(hFind);* *exists2 = ((hFind = ::FindFirstFile(file2, &fd2)) != INVALID_HANDLE_VALUE);* *::FindClose(hFind);* *return (exists1 && exists2 && fd1.nFileSizeLow == fd2.nFileSizeLow);* *}* *Currently the code will declare any two files to be the same*		

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	that have the same size. The author's comment to use a CRC doesn't make much sense, as a byte-by-byte comparison would be more efficient. If this code were ever used, its inaccuracies could lead to wide variety of subsequent errors. While most of the preprocessor directives that remove code correctly use #if 0 as their condition, some use #ifdef XXX. There is no reason that a later programmer should realize that defining XXX will cause blocks of code to be reincluded in the system (causing unpredictable results, at best). We also noticed #ifdef LOUISIANA in the code. Prudent software engineering would recommend a single implementation of the voting software, where individual states or municipalities could have their desired custom features expressed in configuration files."		
20	*"While the system is implemented in an unsafe language (C++), the code reflects an awareness of avoiding such common hazards as buffer overflows. Most string operations already use their safe equivalents, and there are comments reminding the developers to change others (e.g., should really use snprintf). While we are not prepared to claim that there are no buffer overflows in the current code, there are at the very least no glaringly obvious ones. Of course, a better solution would have been to write the entire system in a safe language, such as Java or C#."*	O-34	The scope of the risk assessment did not include a review of Diebold's software engineering practices. However, such an attack vector would require network access. The DRE devices are not connected to a network.
20	*"The core concepts of object oriented programming such as encapsulation are well represented, though in some places C++'s non-typesafe nature is exploited with casts that could conceivably fail. This could cause problems in the future as these locations are not well documented."*	N/A	This is not a security requirement.
20	*"Overall, the code is rather unevenly commented. While most files have a description of their overall function, the meanings of individual functions, their arguments, and the*	M-102	The scope of the risk assessment did not include a review of Diebold's software engineering practices. It should be noted that since the publication of the Rubin report, Diebold has

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	algorithms within are more often than not undocumented."		developed, documented, and implemented a change control process, which has been delivered to the SBE.
21	*"An important point to consider is how code is added to the system. From the CVS logs, we can see that most code updates are in response to specific bugs that needed to be fixed. There are numerous authors who have committed changes to the CVS tree, and the only evidence that we have found that the code undergoes any sort of review process comes from a single log comment: "Modify code to avoid multiple exit points to meet Wyle requirements." This could refer to Wyle Laboratories whose website claims that they provide all manner of testing services."*	M-3	The scope of the risk assessment did not include a review of Diebold's software engineering practices. It should be noted that since the publication of the Rubin report, Diebold has developed, documented, and implemented a change control process, which has been delivered to the SBE.
21	*"There are also pieces of the voting system that come from third parties. Most obviously is the operating system, either Windows 2000 or Windows CE. Both of these OSes have had numerous security vulnerabilities and their source code is not available for examination to help rule out the possibility of future attacks. Besides the operating system, an audio library called "fmod" is used.15 While the source to fmod is available with commercial licenses, unless the code is fully audited there is no proof that fmod itself does not contain a backdoor."*	M-3	Exploitation of these attack vectors would require network access. The DRE devices are not connected to a network.
21	*"Due to the lack of comments, the legacy nature of the code, and the use of third-party code and operating systems, we believe that any sort of comprehensive, top-to-bottom code review would be nearly impossible. Not only does this increase the chances that bugs exist in the code, but it also implies that any of the coders could insert a malicious backdoor into the system. The current design deficiencies provide enough other attack vectors that such*	M-3	The scope of the risk assessment did not include a review of Diebold's software engineering practices. However, such an attack vector requires network access. This risk is mitigated because the DRE devices are not connected to a network.

Page #	Statement from Rubin Report	Ref. to Table 5.8	State of Maryland Controls
	an explicit backdoor is not required to successfully attack the system. Regardless, even if the design problems are eventually rectified, the problems with the coding process may well remain intact."		
21	*"While the code we studied implements a full system, the implementors have included extensive comments on the changes that would be necessary before the system should be considered complete. It is unclear whether the programmers actually intended to go back and remedy all of these issues as many of the comments existed, unchanged, for months, while other modifications took place around them. It is also unclear whether later version of AVTSCE were subsequently created."*	N/A	This is not a security requirement.
22	*"There are, however, no comments that would suggest that the design will radically change from a security perspective. None of the security issues that have been discussed in this paper are pointed out or marked for correction. In fact, the only evidence at all that a redesign might at one point have been considered comes from outside the code: the Crypto++ library16 is included in another CVS archive in cvs.tar. However, the library was added in September 2000 and was never used or updated. We infer that one of the developers may have thought that improving the cryptography would be useful, but then got distracted with other business."*	N/A	This is not a security requirement.

APPENDIX C:TABLE OF INTERVIEWS CONDUCTED DURING THIS REVIEW

In the course of our evaluation of the AccuVote-TS system, SAIC interviewed several people involved with the system with regards to the system, its setup, storage, operations and maintenance. Following is a list of the people interviewed for our review. These interviews were conducted between August 13, and August 18, 2003.

Date	Name	Title	Area
08/13/03	Susan Campbell	IT Specialist	Montgomery County
	Paul Valette	Manager, Election Operations	
08/13/03	Robin Downs	Elections Administrator	Prince George's County
	Hugh Alexander	IT Consultant	
	Alicia Alexander	Assistant to the Administrator	
08/14/03	Julie Och	Chief Judge	Montgomery County
	Paul Valette	Manager, Election Operations	
	Charles Deegan	President BOE	Prince George's County
	Carl Ruble	Vice President BOE	
	John P. Morrissey	Attorney	
	Daniel Lee	Chief Judge	
	Harold Rustin	Manager, Election Operations	
08/15/03	David Heller	Project Manager	SBE
	Tom Feehan	Diebold Engineer	Diebold

~~Date~~	~~Name~~	~~Title~~	~~Area~~
~~08/18/03~~	~~Donna Duncan~~	~~Director~~	~~SBE~~
	~~Pam Woodside~~	~~CIO~~	~~SBE~~

~~APPENDIX D:~~APPENDIX C: TABLE OF DOCUMENTS REVIEWED DURING THIS ASSESSMENT

In the course of our evaluation of the AccuVote-TS system, SAIC reviewed all available documentation pertaining to the system, its setup, storage, operations and maintenance. Following is a list of the documents considered in our review. The document review commenced on August 5, and was completed August 20, 2003.

File Name if Electronic	Actual Title
2002 AG Instructions DRE	INSTRUCTIONS OF THE ATTORNEY GENERAL OF MARYLAND TO THE REGISTERED VOTERS OF MARYLAND FOR THE OPERATION OF ACCUVOTE – TS VOTING UNITS
2002 AG Instructions Writein	INSTRUCTIONS FOR WRITE-IN VOTES
2002 Allegany County Manual	ELECTION JUDGES TRAINING AND PROCEDURES
2002 general probs (must be AG)	N/A
4-30-03i	DRE Open Issues
05-14-03i	DRE Open Issues
05-21-03i	DRE Open Issues
05-07-03i	DRE Open Issues
09-15-02p	RECOMMENDATIONS GUBERNATORIAL PRIMARY ELECTION 2002

File Name if Electronic	Actual Title
	MONTGOMERY COUNTY
AGTouchScreen	INSTRUCTIONS OF THE ATTORNEY GENERAL OF MARYLAND TO THE REGISTERED VOTERS OF MARYLAND FOR THE OPERATION OF ACCUVOTE – TS VOTING UNITS
AGWrite-In	INSTRUCTIONS FOR WRITE-IN VOTES
AlleganyGeneralFlowChart	Ballot Creation Process for Allegany County
Codeof Conduct	CODE OF CONDUCT FOR VOTER EDUCATION FACILITATORS
CommPlan	SBE Communications Plan
ContractMod	INFORMATION TECHNOLOGY CONTRACT MODIFICATIONS SBE Voting System Implementation Project State Board of Elections (SBE) PROGRAM
DorchesterGener...	Ballot Creation Process for Dorchester County
DRIMPlan	SBE Disaster Recovery and Incident Management Plan
DRIMTemplate	Disaster Recovery and Incident Management Plan
Export	General Election Results Export Procedure
FinalChangeControl	SBE Change Control Plan
FinalMaintenancePlan	SBE Maintenance Plan
How to Configure a TS to Transfer Results	How to Configure a TS to Transfer Result

File Name if Electronic	Actual Title
ImplementationPlan	SBE Implementation Plan
Judge's TS What If's	AccuVote TS - Technician's What If's
L&Acertificate1	CERTIFICATION # 1 (Inspector) ACCUVOTE TS PRE-ELECTION LOGIC AND ACCURACY TESTING
L&Acertificate2	CERTIFICATION # 2 (Inspector) ACCUVOTE TS PRE-ELECTION LOGIC AND ACCURACY TESTING
L&Acertificate3	CERTIFICATION # 3 (Inspector) ACCUVOTE TS PRE-ELECTION LOGIC AND ACCURACY TESTING
L&Acertificate4	CERTIFICATION # 4 (Inspector) ACCUVOTE TS PRE-ELECTION LOGIC AND ACCURACY TESTING
L&Acertificate5	CERTIFICATION # 5 (Inspector) ACCUVOTE TS PRE-ELECTION LOGIC AND ACCURACY TESTING
L&AChecklist	AccuVote-TS L&A Checklist
L&ADeclaration	BOARD OF ELECTIONS COMPUTER PROFESSIONAL DECLARATION AND CONFIDENTIALITY AGREEMENT
MontgomerGeneralFlowChart	Ballot Creation Process for Montgomery County
PCMCIA.Recovery	Election Recovery PCMCIA Failure Election in Progress
Performing the LA pre-election setup checks	L&A Testing Revised 10/09/02
PhaseII_IP	State Board of Elections, AccuVote Touch Screen Voting System Phase II Implementation Plan June 19, 2003
PollworkerManual	WELCOME TO DIEBOLD POLL WORKER TRAINING

File Name if Electronic	Actual Title
PowerManagementPlan	State Board of Elections, AccuVote Voting System Power Management Plan
PrinceGeorgeGeneralFlowChart	Ballot Creation Process for Prince George's County
QAPlan	State Board of Elections Systems Project Management Office Support Quality Assurance (QA) Plan
RISCPlan	State Board of Elections Systems Project Management Office Support Risks, Issues, Systems Incidents, and Changes (RISC) Plan
Software_Hrdwr Changes	Software/Hardware Changes to Diebold Elections Systems
SpaceRequirements4-03	PHASE II IMPLEMENTATION SPACE AND ELECTRICAL REQUIREMENTS BY COUNTY
TECHNICIANS Election Day Check Lists	TECHNICIANS' MORNING CHECK LIST
Tech's TS What If's	AccuVote TS - Technician's What If's
TS UNIT DEFECT BREAKDOWN	TS UNIT DEFECT BREAKDOWN
TSAccumulate	Using the AccuVote TS
TSAccumulateNoWrite	Using the AccuVote TS
TSClose	Using the AccuVote TS
TSModem	Using the AccuVote TS
TSOpen	Using the AccuVote TS
TSVIBS	Using the AccuVote TS
VCProgrammer 4.1 User's Guide Revision 3.0	VC Programmer Guide 4.1

File Name if Electronic	Actual Title
Voter Card Encoder User's Guide Revision 1.3	Voter Card Encoder User Guide
VoterAccessCard	Front side of card
WarehouseStandard4-03	Diebold Warehouse Standards
WBSPlan	WBS Plan
20981KeyboardAttachment-20040211	Santa Clara RFP
checksandbalances	July 30, 2003 Diebold - Checks and balances in elections equipment and procedures prevent alleged fraud scenarios
diebold JHU Study	Analysis of an Electronic Voting System Aviel. D. Rubin, et al, July 23, 2003
georgia	Security in the Georgia Voting System Britain J. Williams, Ph.D. April 23, 2003
	Board of Election – PG County 2002 Voting Machine Technician's Guide
	Board of Election – PG County 2002 Quick Reference Guide
	Procedures for Official Canvass, Verification and Post-Election Audit
	Allegany County – AccuVote Manual
	SBE Procedures for Election Day
	Diebold – AccuVote-TS R6 1.2

File Name if Electronic	Actual Title
	Diebold – Election Administrator's Guide
	Diebold – Ballot Station 4.3 User's Guide
	Diebold – Voting System – Phase II Election Judge Manual
	Precinct Count 1.96 User's Guide , Revision 2.0, Diebold Election Systems
	Wyle Test Report, Change Release Report of the Accuvote-TS R6 DRE Voting Machine (Firmware Change Release 4.3.15)
	Diebold Election Systems Software Qualification test Report GEMS 1-18, Addendum 2, 7/08/03, Ciber, Inc.
	Memo from Lamone – 2002 Election Results Transfer
	State-Wide Voting System Project Election Night Report Procedures
	SBE Recount Process Workflow for the AccuVote Voting System
	Auditability of Non-Ballot, Poll-Site Voting Systems
	Part II. Position Functions
	Procedures for Official Canvass Verification and Post-Election Audit
	Memorandum Election Day Log
	Registration & Election Laws of MD
	DRE Voting System Contact
	MD Certification Evaluation of the Global Election Systems, Inc AccuTS R6
	Diebold – Poll Worker Training

File Name if Electronic	Actual Title
	SBE Work Breakdown Structure
	SBE Communication Plan
	SBE Risks, Issues, System Incidents & Changes
	Registration and Election Laws of Maryland
	Diebold Pollworker's Guide
	Election Judges Training & Procedures
	Diebold AccuVote-TS R6 Hardware Guide
	Diebold – User's Guide
	SBE – Phase II Implementation Plan
	Information Technology Contract Modifications
	Recommendations Gubernatorial Primary Election 2002
	Memorandum Emergency Contingency Plan
	Gubernatorial General Election Night Results Processing, September 10, 2002
	Gubernatorial General Election Night Results Processing, November 5, 2002
	2002 Gubernatorial Primary Election Results Tracking Worksheet
	2002 Gubernatorial General Election Results Tracking Worksheet
	2002 Gubernatorial General Election SBE Staffing Worksheet
	State-Wide Voting System Project General Election Results Export Procedures

File Name if Electronic	Actual Title
	Board of Election – PG County 2002 Election Judge Manual
	Prince George's County Government, Office of Information Technology and Communications, Letter to Linda Lamone, Administrator, Regarding Concerns and Recommendation on Accuvote –TS systems.
	Diebold Poll Worker Training Guide
	SBE AccuVote-TS Direct Recording Electronic Voting System Certification
	State-Wide Voting System Project, Touchscreen and Booth Acceptance Test Guide
	State-Wide Voting System Project, UPS Acceptance Test Guide
	State-Wide Voting System Project, OS Acceptance Test Guide
Diebold Source Code, version 4.3.1.5	Diebold Source Code, version 4.3.1.5, received 15 August 2003
CD	PG County – Taking Charge Election Judge Training
CD	Montgomery County – Training Materials Election Judge & Tech. Staff
CD	Montgomery Judge's Manual Complete
Video	"From Chads to Bytes"

Documentation Received After – Wed-08/14

File Name if Electronic	Actual Title

File Name if Electronic	Actual Title
GA – Certification Test Report 2003	Certification Test of GA
GA – LCCR Analysis – Voter Verification	*ELECTION REFORM POLICY ANALYSIS:* "Voter-Verified Paper Trails" Are Not Needed To Keep Elections From Being Stolen
GA – Security – 08	Security Features of Georgia's Electronic Voting System
GA – Voting system security	Security in the Georgia Voting System (duplicate)