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

EXECUTIVE SUMMARY ..... **III**

Findings & Recommendations iii

1. INTRODUCTION **1**

1.1. Overview 1
1.2. Purpose 1
1.3. Scope 1
1.4. Document Organization 2

2. MAJOR RISKS AND MITIGATION STRATEGIES **3**

2.1. Management Controls 3
2.1.1. AccuVote-TS voting system is not compliant with State of Maryland Information Security Policy & Standards 3
2.1.2. SBE has not ensured the integrity of the AccuVote-TS voting system 4
2.1.3. SBE has not created a System Security Plan 4
2.1.4. SBE does not require the secure transmission of election vote totals 5
2.1.5. SBE does not require the review of the computer audit trails 5
2.1.6. The AccuVote-TS voting system training does not include an information security component 5
2.1.7. SBE does not require a review of security controls after significant modifications are made to the AccuVote-TS voting system 6
2.1.8. ~~Controls are not implemented to detect~~ Unauthorized transaction attempts by authorized and/or unauthorized users 6
2.1.9. No documentation currently exists regarding appropriate access controls to the AccuVote-TS voting system 7
2.2. Operational Controls 7
2.2.1. SBE relies upon Diebold (the AccuVote-TS vendor) to load the version of software certified by the Independent Test Authority (ITA) 7
2.2.2. SBE GEMS server is connected to the SBE intranet 7
2.3. Technical Controls 8
2.3.1. Audit logs are not configured properly, and are not reviewed 8
2.3.2. GEMS server configuration is not compliant with State of Maryland Information Security Policy & Standards for identification and authentication 9
2.3.3. ~~GEMS server user session never times out and allows unlimited password guessing~~ .9
2.4. Review of Rubin Report 9
2.5. Overall Risk Rating 10

3. RISK ASSESSMENT METHODOLOGY AND APPROACH **11**

3.1. Assumptions 11
3.2. Methodology and Approach 12
3.2.1. Step 1: Characterize the **AccuVote-TS Voting System** 12
3.2.2. Step 2: Perform Threat Identification 13
3.2.3. Step 3: Perform Vulnerability Identification 13
3.2.4. Step 4: Perform Controls Analysis 13

3.2.5. Step 5: Determine Threat Likelihood 14
3.2.6. Step 6: Perform Impact Analysis 14
3.2.7. Step 7: Determine Level of Risk 14
3.2.8. Step 8: Develop Risk Mitigation Strategies 15
3.2.9. Step 9: Document Results 15

4. ACCUVOTE-TS CHARACTERIZATION, STEP 1 16

4.1. Functional Description of the **AccuVote-TS** 16
4.2. AccuVote-TS System and Interfaces 17
4.3. System Users 18
4.3.1. Internal Users 18
4.3.2. External Users 18
4.3.3. Special Processing IDs 19

~~**5. RISK ASSESSMENT RESULTS, STEPS 2-9 ..... 20**~~

~~5.1. Step 2 - Threat Identification ..... 20~~
~~5.2. Step 3 - Vulnerability Identification ..... 21~~
~~5.3. Step 4 - Controls Analysis ..... 21~~
~~5.3.1. Management Controls Analysis ..... 21~~
~~5.3.2. Operational Controls Analysis ..... 24~~
~~5.3.3. Technical Controls Analysis ..... 26~~
~~5.4. Step 5 - Likelihood Definition ..... 27~~
~~5.4.1. Likelihood Rating Rationale ..... 27~~
~~5.5. Step 6 - Impact Analysis ..... 27~~
~~5.5.1. Impact Rating Rationale ..... 28~~
~~5.6. Step 7 - Risk Determination ..... 28~~
~~5.7. Detailed Risk Assessment Results ..... 30~~

APPENDIX A: ACRONYMS A-1

APPENDIX B: SECURITY STATEMENTS FROM THE RUBIN REPORT & STATE OF MARYLAND CONTROLS B-1

~~**APPENDIX C: TABLE OF INTERVIEWS CONDUCTED DURING THIS REVIEW ..... B-1C-1**~~

APPENDIX D: TABLE OF DOCUMENTS REVIEWED DURING THIS ASSESSMENT C-1~~D-1~~

LIST OF FIGURES

Figure 3-1: Risk Assessment Methodology and Approach 12
Figure 4-1: AccuVote-TS High-Level Infrastructure and Connectivity 17
~~Figure 5-1: State of Maryland Threat Sources ..... 21~~

LIST OF TABLES

~~Table 5-1: Management Controls ..... 22~~

~~Table 5-2: Operational Controls ..... 24~~
~~Table 5-3: Technical Controls ..... 26~~
~~Table 5-4: Likelihood Definition ..... 27~~
~~Table 5-5: Magnitude of Impact Definition ..... 28~~
~~Table 5-6: Risk Rating/Implementation Correlation ..... 29~~
~~Table 5-7: Quantitative Risk Rating ..... 29~~
~~Table 5-8: Requirement/Threat Source/Likelihood/Impact/Risk Rating/Mitigation ..... 31~~

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.

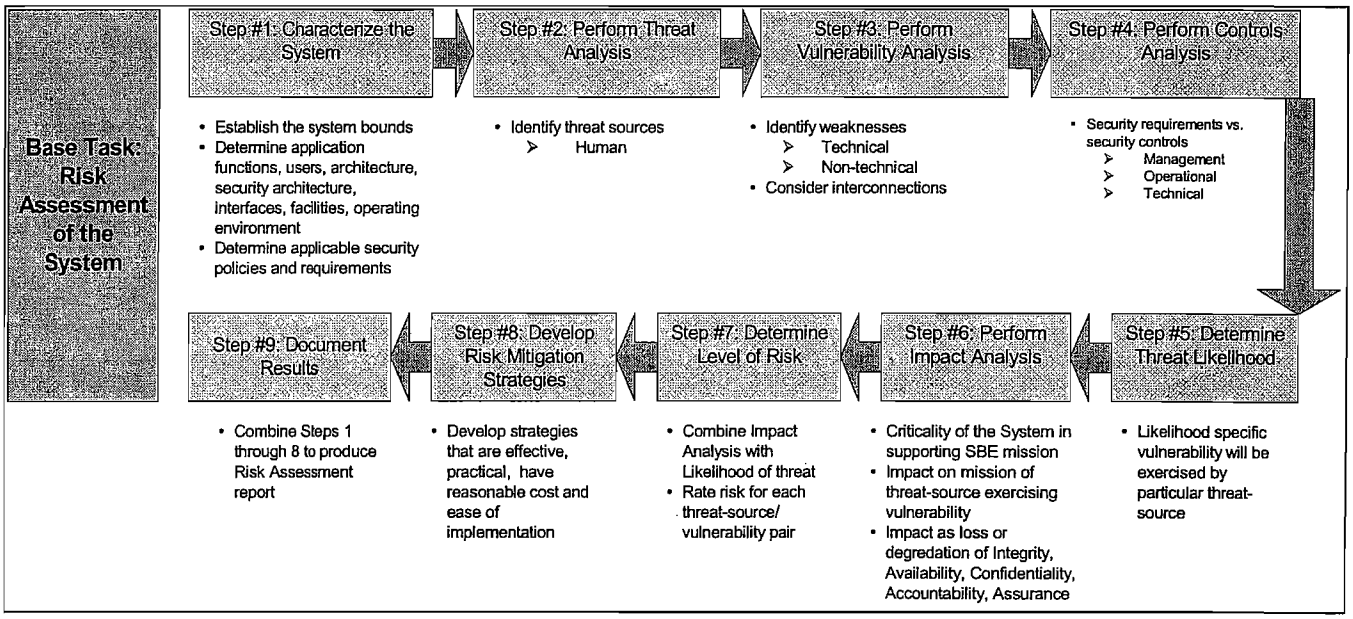


Figure 3-1: Risk Assessment Methodology and Approach

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.

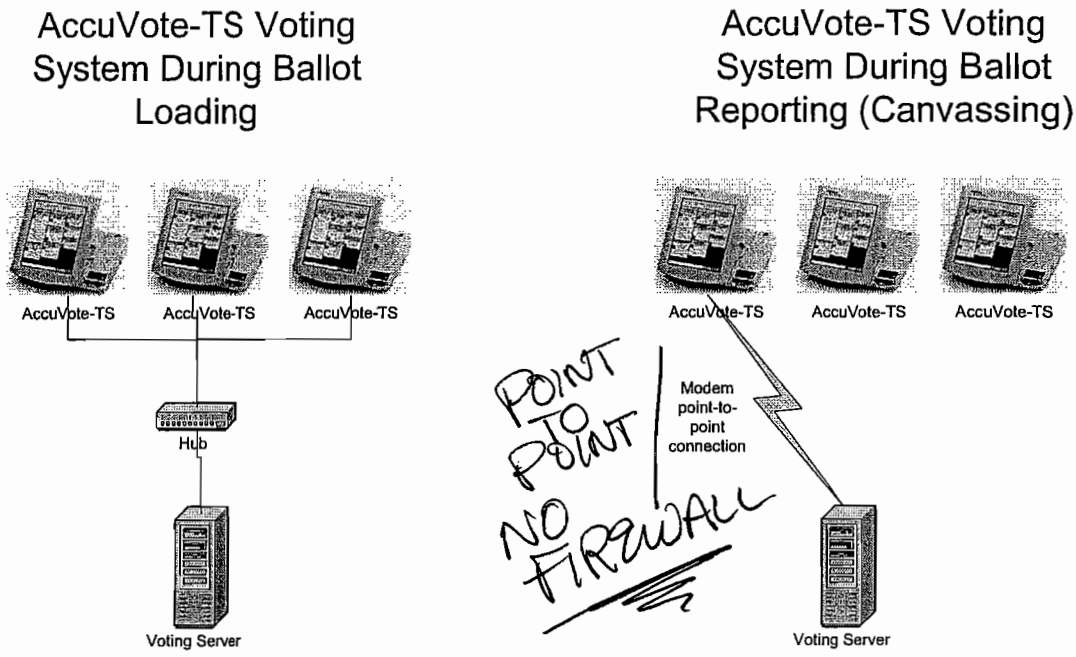


Figure 4-1: AccuVote-TS High-Level Infrastructure and Connectivity

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~~

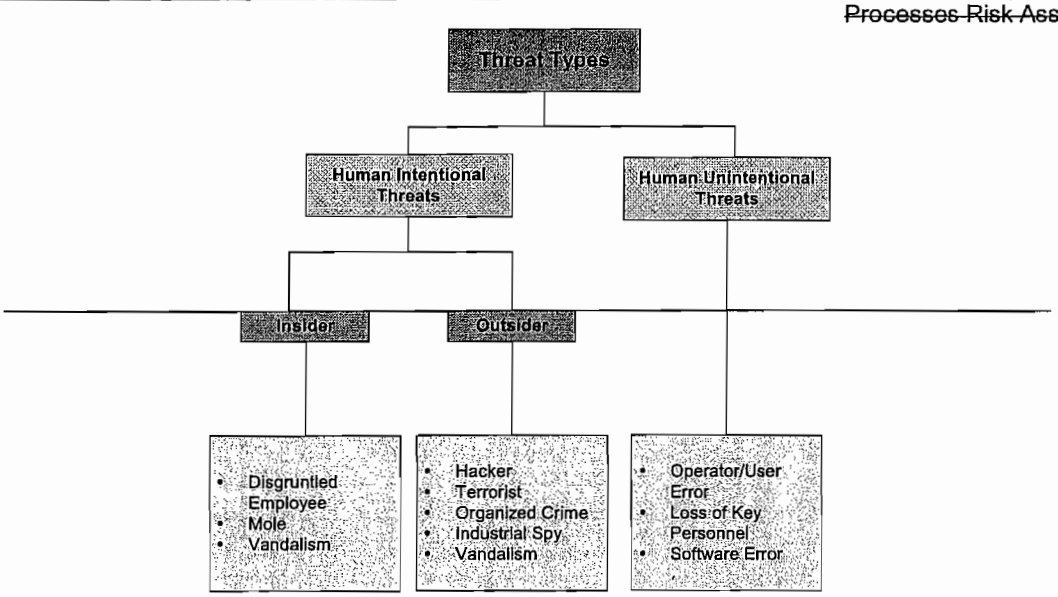
~~This section provides the findings of the risk assessment, following Steps 2 through 9 of the risk assessment methodology. The results are provided in tabular form. Each of the vulnerabilities is:~~

- ~~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.~~		