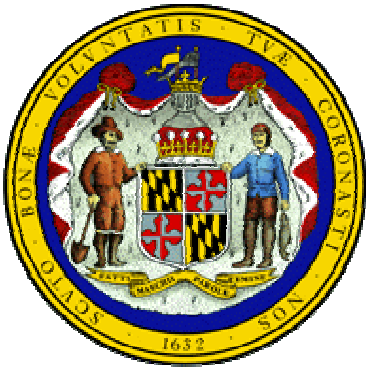

State of Maryland

Risk Assessment Report

Diebold AccuVote-TS Voting System and Processes

September 2, 2003

Science Applications International Corporation
An Employee-Owned Company

SAIC-6099-2003-261

Prepared for:
Department of Budget and Management
Office of Information Technology
45 Calvert Street
Annapolis, MD 21401

This page is intentionally blank.

EXECUTIVE SUMMARY

This report presents the results of a risk assessment of the AccuVote-TS voting system as currently implemented in Maryland by the State Board of Elections (SBE) and the Local Boards of Elections (LBEs). This Risk Assessment report includes evaluations of threats, vulnerabilities, security controls, and risks associated with the AccuVote-TS system and possible impacts to the State and the integrity of its elections process from successful exploitation of identified weaknesses.

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 fully formed and documented, correctly implemented, and effective in their application.

Findings & Recommendations

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. In general, SAIC made many of the same observations, *when considering only the source code.* While many of the statements made by Mr. Rubin were technically correct, it is clear that Mr. Rubin did not have a complete understanding of the State of Maryland's implementation of the AccuVote-TS voting system, and the election process controls or environment. 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. 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.

This Risk Assessment has identified several high-risk vulnerabilities in the implementation of the managerial, operational, and technical controls for AccuVote-TS voting system. If these vulnerabilities are exploited, significant impact could occur on the accuracy, integrity, and availability of election results. In addition, successful exploitation of these vulnerabilities could also damage the reputation and interests of the SBE and the LBEs. This Risk Assessment also identified numerous vulnerabilities with a risk rating of medium and low that may have an impact upon AccuVote-TS voting if exploited.

This assessment of the current 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. 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.
- 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). **[Redacted]**

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

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

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

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

[Redacted]

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. **[Redacted]**

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. **[Redacted]** 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.

2.1.8. [Redacted]

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.

[Redacted]

[Redacted]

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. **[Redacted]**

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. **[Redacted]**

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. **[Redacted]**

[Redacted]

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. **[Redacted]**

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

[Redacted]

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.

[Redacted] 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

[Redacted]

[Redacted]

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. **[Redacted]**

2.3.3. [Redacted]

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.

[Redacted]

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.

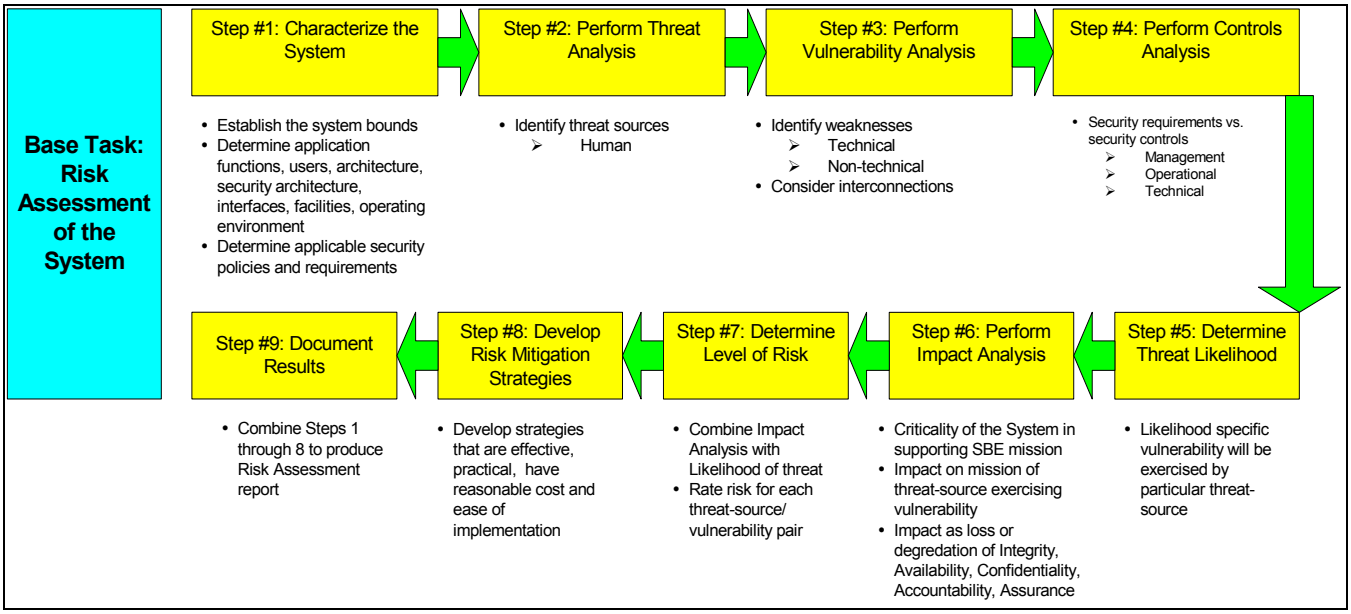

Figure 3-1: Risk Assessment Methodology and Approach

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.

[Redacted]

[Redacted]

Figure 4-1: [Redacted]

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 **[Redacted]** as its operating system. The currently used version of the AccuVote-TS software is **[Redacted]** 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.

[Redacted] 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 **[Redacted]** 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. **[Redacted]** All other times, the voting terminal operates in a stand-alone mode.

[Redacted]

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.

5. [REDACTED]

APPENDIX A: ACRONYMS

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

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

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

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

(This document is available as a separate file)

APPENDIX C: [REDACTED]

APPENDIX D: TABLE OF DOCUMENTS REVIEWED DURING THIS ASSESSMENT

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

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

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

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

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

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

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

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

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

Documentation Received After – Wed-08/14

File Name if Electronic	Actual Title

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