Ohio Secretary of State

Office of J. Kenneth Blackwell

Direct Recording Electronic (DRE) Technical Security Assessment Report

November 21, 2003

COMPUWARE

Compuware Corporation

1103 Schrock Road, Suite 205

Columbus, Ohio 43229

(614) 847-8212

*** Confidential ***

This page intentionally left blank.

Table of Contents

PART ONE: EXECUTIVE SUMMARY 1
Introduction 1
Work in Scope 4
Methodology and Approach 6
Platform Review 7
Code Review 8
DRE System Interfaces and Tasks 9
Work Flow/Process Model 11
Environment 13
Hardware Configuration 13
Software Configuration 14
Requirements Identified 16
Test Scenarios 16
Risks Identified 17
Potential Vulnerabilities & Recommended Mitigation Strategies 17
Conclusion 20
PART TWO: DIEBOLD 21
Overview 21
Step 1: Characterization of the AccuVote-TS Voting System 21
AccuVote-TS System Interfaces 22
Work Flow / Process Model 24
Environment 27
Hardware Configuration 27
Software Configuration 27
Network Configuration 28
Step 2: Threat Identification 29
Step 3: Vulnerability Identification 30
Requirements Tested & Test Results 30
Test Areas 30
Specific Tests and Test Results 30
Step 4: Controls Analysis 49
Step 5: Threat Likelihood 50
Step 6: Impact Analysis 51
Step 7: Determine Risks 53
Risks Identified 53
Risk Levels of Identified Risks 70
Step 8: Risk Mitigation Strategies 73
Recommended Risk Mitigation Strategies 73
Code Review 73
Platform Review 75
Physical Testing 76
Step 9: Document Results 77
Conclusion 78

PART THREE: ES&S 81
Overview 81
Step 1: Characterization of the iVotronic Voting System 81
iVotronic System Interfaces 82
Work Flow / Process Model 84
Environment 87
Hardware Configuration 87
Software Configuration 87
Network Configuration 88
Step 2: Threat Identification 89
Step 3: Vulnerability Identification 90
Requirements Tested & Test Results 90
Test Areas 90
Specific Tests and Test Results 90
Step 4: Controls Analysis 107
Step 5: Threat Likelihood 108
Step 6: Impact Analysis 109
Step 7: Determine Risks 110
Risks Identified 110
Risk Levels of Identified Risks 127
Step 8: Risk Mitigation Strategies 130
Recommended Risk Mitigation Strategies 130
Code Review 130
Platform Review 131
Physical Testing 132
Step 9: Document Results 134
Conclusion 135
PART FOUR: HART INTERCIVIC 137
Overview 137
Step 1: Characterization of the eSlate 3000 Voting System 137
eSlate 3000 System Interfaces 138
Work Flow / Process Model 140
Environment 143
Hardware Configuration 143
Software Configuration 143
Network Configuration 144
Step 2: Threat Identification 145
Step 3: Vulnerability Identification 146
Requirements Tested & Test Results 146
Test Areas 146
Specific Tests and Test Results 146
Step 4: Controls Analysis 162
Step 5: Threat Likelihood 163
Step 6: Impact Analysis 164
Step 7: Determine Risks 166

Risks Identified 166
Risk Levels of Identified Risks 182
Step 8: Risk Mitigation Strategies 184
Recommended Risk Mitigation Strategies 184
Code Review 184
Platform Review 185
Physical Testing 186
Physical Testing 187
Step 9: Document Results 187
Conclusion 187
PART FIVE: SEQUOIA 189
Overview 189
Step 1: Characterization of the AVC Edge Voting System 189
AVC Edge System Interfaces 190
Work Flow / Process Model 192
Environment 195
Hardware Configuration 195
Software Configuration 195
Network Configuration 195
Step 2: Threat Identification 196
Step 3: Vulnerability Identification 197
Requirements Tested & Test Results 197
Test Areas 197
Specific Tests and Test Results 197
Step 4: Controls Analysis 215
Step 5: Threat Likelihood 216
Step 6: Impact Analysis 217
Step 7: Determine Risks 219
Risks Identified 219
Risk Levels of Identified Risks 237
Step 8: Risk Mitigation Strategies 240
Recommended Risk Mitigation Strategies 240
Code Review 240
Platform Review 241
Physical Testing 242
Step 9: Document Results 243
Conclusion 244
ATTACHMENT A: Risk Assessment Methodology A-1
ATTACHMENT B: Glossary B-1
ATTACHMENT C: Documents Referenced C-1

This page intentionally left blank.

PART ONE: EXECUTIVE SUMMARY

Introduction

The Ohio Secretary of State (SOS) hired Compuware Corporation to conduct an extensive security assessment and validation of the Direct Recording Electronic (DRE) voting machines from four vendors who were qualified by the SOS to help upgrade the state's voting systems as required by the Help America Vote Act of 2002 (HAVA):

- AccuVote-TS from Diebold Election Systems
- iVotronic from Election Systems and Software (ES&S)
- eSlate 3000 from Hart InterCivic
- AVC Edge from Sequoia Voting Systems

In order to ensure the integrity of this assessment, the SOS and Compuware set up a secure, real-world testing environment at the State of Ohio Computer Center (SOCC). Compuware obtained the hardware and software to be tested from each vendor, and set up the equipment in a secure, locked room at the SOCC facility. The assessment team then used this hardware and software to conduct hands-on testing and evaluations.

In this technical security assessment, Compuware tested the following hardware and software from each vendor.

Vendor	Hardware	Software
Diebold Election Systems	• AccuVote-TS R6, Firmware version 4.3.15 • Voter Card Encoder version 1.1.4	Global Election Management System (GEMS) version 1.18.18
Election Systems and Software (ES&S)	iVotronic version 7.4.5.0	Unity Election System (UES) software version 2.2
Hart InterCivic	• eSlate 3000 version 2.1 • Judge's Booth Controller (JBC) version 1.16	• BOSS Election Management Software version 2.9.04 • TALLY software version 2.9.08 • SERVO software version 1.0.2
Sequoia Voting Systems	• AVC Edge version 4.1. D • Card Activator version 4.2	• WinEDS Election Management Software version 2.6

Continued on the next page

Introduction (continued)

Compuware conducted a technical review and test of the source code, operating systems, and hardware platforms of the DRE's. This report details the steps used to assess the DRE's and presents the findings of the technical assessment, including an evaluation of the risks and vulnerabilities that were discovered. The report identifies:

- Requirements tested
- Test scenarios used
- Test results
- Risks identified
- Likelihood and impact of identified risks
- Risk mitigation strategies
- Recommendations

In addition to Compuware's focus on technical assessment, independent consulting firms InfoSENTRY and RJV Consulting are participating in the security assessment. Their roles are listed below.

- InfoSENTRY is conducting an evaluation of the administrative policies and procedures utilized by the voting system vendors to ensure that security is built in and maintained in their voting systems, and evaluating the state's administrative processes; and will provide a deliverable that summarizes both InfoSENTRY's findings and Compuware's findings, and will include recommendations for going forward.
- RJV Consulting is serving in an advisory capacity, including report review and identification of issues that may need addressed in the procurement contract process.

Continued on the next page

Introduction (continued)

The following diagram shows the division of responsibilities for the overall security assessment.

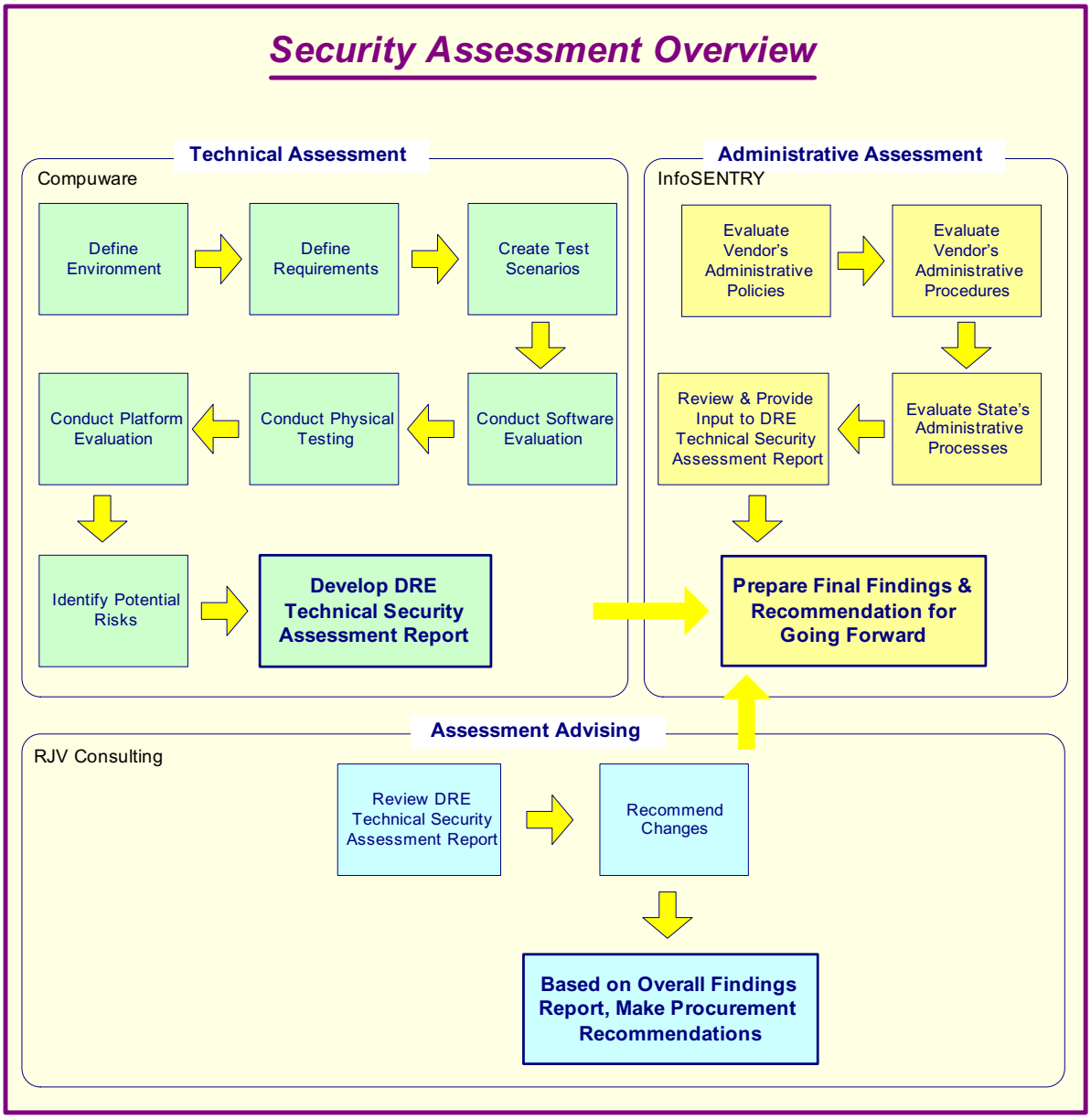

Figure 1 – *Security Assessment Overview*

Work in Scope

The scope of this effort was to provide a Security Assessment for the following DRE voting machines:

- AccuVote-TS from Diebold Election Systems
- iVotronic from Election Systems and Software (ES&S)
- eSlate 3000 from Hart InterCivic
- AVC Edge from Sequoia Voting Systems

In each case, the scope is limited to the various hardware and software components of the DRE plus any data input or output streams which service the DRE. For example, we investigated the transfer of the ballot definition data from the respective election management software programs to the DRE, but we did not investigate the election management application itself.

The assessment was conducted on the hardware and software versions currently approved by the Ohio Board of Voting Machine Examiners for use in Ohio. Although some of the vendors have more recent versions that they have or will be submitting for approval, these more recent products were not evaluated because they are currently not certified for use in the State of Ohio.

Continued on the next page

Work in Scope (continued)

Compuware tested the following hardware and software in this technical security assessment:

Vendor	Hardware	Software
Diebold Election Systems	• AccuVote-TS R6, Firmware version 4.3.15 • Voter Card Encoder version 1.1.4	Global Election Management System (GEMS) version 1.18.18
Election Systems and Software (ES&S)	iVotronic version 7.4.5.0	Unity Election System (UES) software version 2.2
Hart InterCivic	• eSlate 3000 version 2.1 • Judge's Booth Controller (JBC) version 1.16	• BOSS Election Management Software version 2.9.04 • TALLY software version 2.9.08 • SERVO software version 1.0.2
Sequoia Voting Systems	• AVC Edge version 4.1. D • Card Activator version 4.2	• WinEDS Election Management Software version 2.6

The following tasks were within the scope of Compuware's assessment.

- Defined environment of DRE – Identified the components of the DRE and all data streams that service the DRE.
- Defined requirements of DRE – Identified and documented the requirements that DRE's must meet to operate in a secure environment.
- Created test scenarios – For each specific DRE, wrote test scenarios designed to reveal whether the security requirements above were met by the DRE.
- Conducted platform review of DRE – Reviewed the hardware, design documentation, and other vendor information to determine potential security risk areas. Use of removable media, network ports, access controls, and input devices were evaluated.
- Conducted software code review of DRE – Reviewed the software, design documentation, and other vendor information to determine potential security risk areas. Use of encryption, checksums, and passwords were evaluated. Code was also reviewed for existence of software engineering discipline.
- Conducted physical testing of DRE – Test scenarios were executed and results captured.
- Identified and evaluated potential risks of DRE – Based on the results of the code review, platform review, and physical testing, a list of risks was documented and evaluated for likelihood and severity.
- Identified mitigating strategies – The assessment team recommended solutions that are intended to mitigate or eliminate the risks identified. The goal of the recommended risk mitigation strategies was to reduce the level of risk to the electronic voting system and its data to an acceptable level.

Methodology and Approach

This assessment was performed based on the methodology documented in National Institute of Standards and Technology (NIST) SP 800-30, *Risk Management Guide for Information Technology Systems*.

The diagram below illustrates the methodology used. (Refer to Attachment A of this document for a detailed explanation of the methodology.)

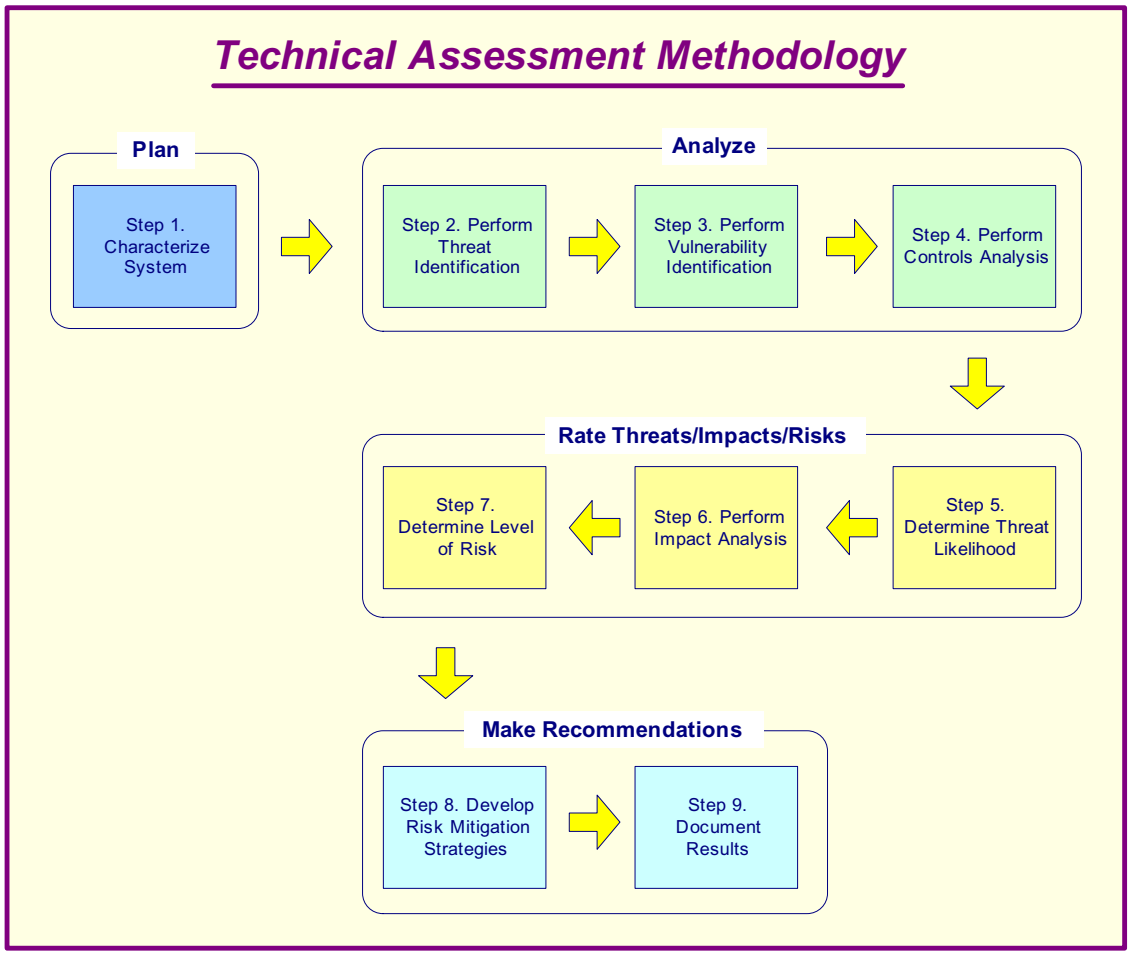

Figure 2 – *Technical Assessment Methodology*

Platform Review

This section describes the approach that was followed in the Platform Review portion of the technical security assessment.

1. Analyzed and Documented

The security assessment began by making an analysis of the components that comprise the system. Detailed information was collected through study, analysis, product literature, Question and Answer sessions with vendors, and hands-on observations of the product.

a. Characterized the system through study and analysis of all the physical and logical components of each system.
b. Performed reviews, demonstrations, and Question and Answer sessions with vendors.
c. Documented details and initial findings.

2. Identified and Scheduled Tasks

Plans were defined and tasks were scheduled to identify potential risks in the system.

a. Reviewed details and findings, then mapped out a task trail or procedural methodology based on specification details.
b. Assigned tasks in a project plan.

3. Performed Scans of Hardware and Network Components

Implementing the assigned tasks was specific to each vendor's product or system. Scans were conducted on only one system at a time. Scan implementation proceeded in a logical manner that was defined by the make-up of the system.

a. Defined a scan policy for each target or system.
b. Performed or estimated site reconnaissance analysis.
c. Performed threat identification.
d. Performed vulnerability scans and identification.
e. Performed network scans and identification.
f. Performed exploitation analysis.
g. Documented findings and impact analysis.
h. Performed cryptographic analysis.

4. Rated Threats/Impacts/Risks

Compiled and assimilated the collected information. Conducted reviews and performed analysis. Documented initial findings and determined threat likelihood, levels of risk, and impact analysis.

a. Analyzed security loopholes.
b. Determined the threat likelihood.
c. Performed impact analysis.
d. Determined level of risk.

5. Made Recommendations and Suggestions

Compiled and documented overall results and findings. Developed risk mitigation strategies. Submitted recommendations and suggestions.

a. Documented results.
b. Developed risk mitigation strategies.
c. Made suggestions and recommendations.
d. Submitted reports.

Methodology and Approach (continued)

Code Review

This section describes the approach that was followed to perform the Code Review portion of the technical security assessment.

1. Reviewed for Standard Programming Practices

   The vendor-supplied source code was visually reviewed to make sure it followed industry standard programming practices. The review checked to see if a consistent pattern was followed in having descriptive code comments, and if consistent and self-describing naming conventions were used for variables, modules, and constants. The code should have been broken into separate modules or classes and each module should have had functions that perform specific tasks to make it readable and easy to follow.

2. Reviewed Security Features and Error-Handling Logic

   The code should have also implemented security features such as password protection for critical pieces of the vendor software. A review was done to see if industry standard encryption techniques were employed to protect critical data (ballot information, vote record and audit trail) in voting systems and while transferring them across a network to other software systems. The code was also reviewed to see if proper error handling logic had been added consistently throughout the code so that the systems were stable in the event of an error and sufficient information on the state of the system was recorded for future debugging purposes. Code was checked to see if the vote data was stored in multiple locations so that information could be recovered in case of a system disaster. The review also focused on whether industry standard checks had been implemented in the code to make sure the data was not corrupted.

3. Reviewed Database and Third Party Code/Security

   The data model and any database code supplied were also reviewed to see if referential integrity of the database was maintained, and to assess the security levels implemented for database access at the application level. Attention was paid to any third party components used in the applications, as their use requires strict guidelines, security standards and version control. All third party code supplied by the vendors was reviewed to make sure it did not have code providing additional functionality other than what was needed and that it adhered to the security standard of the application.

4. Reviewed Documentation

   The scope of the code review included reviewing the documentation associated with the applications. The requirements documents, system and code design documents, and technical code documents were reviewed to analyze the relationship between code modules and functional requirements of the application. For example, requirements should have been closely tied to modules for easier code management; changes in requirements should have been easily pointed to specific code modules that required modifications.

Note: Given the short time frame of the project, it was not possible to review every single line of code in all of the applications. Review of the code was done using a sampling of code files from these applications. Analysis from the sampling of code files was extrapolated to the overall architecture of the applications.

DRE System Interfaces and Tasks

The following diagram provides a graphical overview of the connections to the DRE. The diagram shows the input/output connections between the DRE and external entities such as the BOE's and voters. The context diagram helps to define the scope of the voting system and the related voting processes and becomes the top level of the analysis hierarchy.

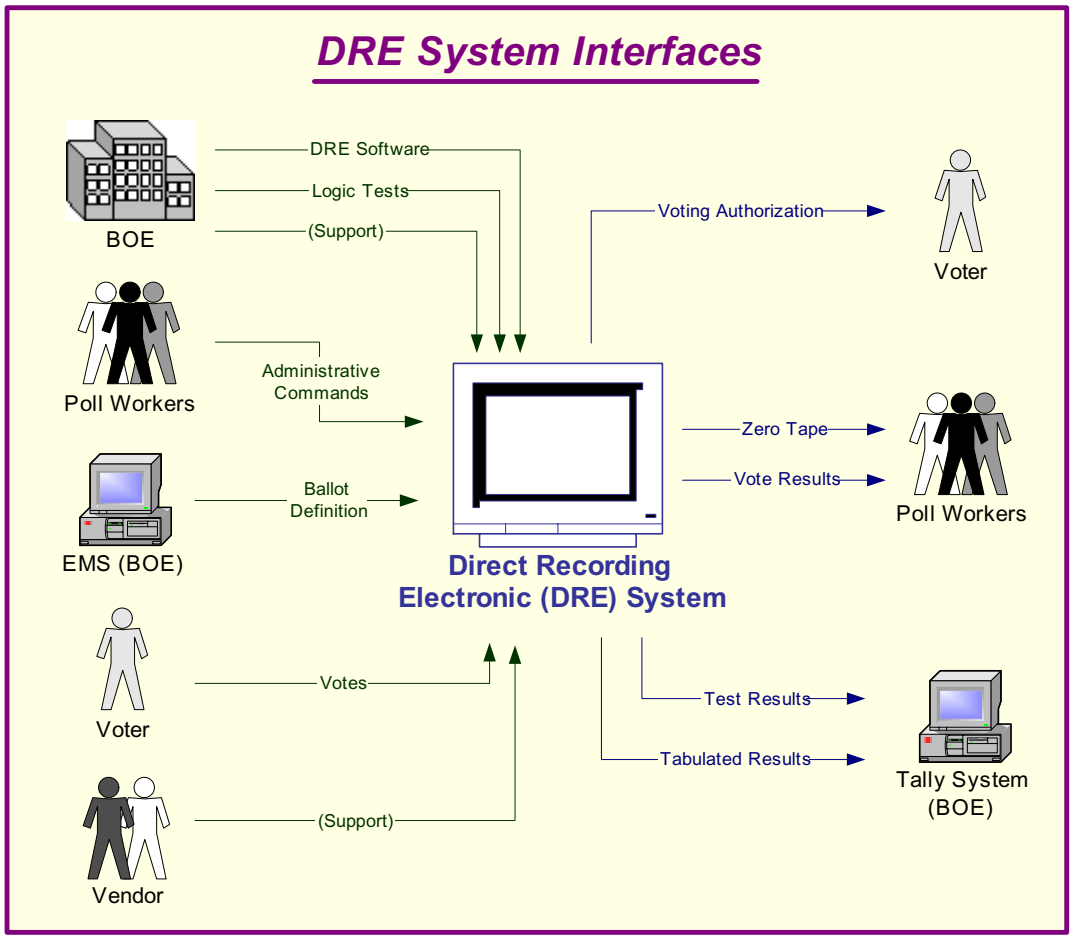

Figure 3 – *DRE System Interfaces*

Continued on the next page

DRE System Interfaces and Tasks (continued)

Following is an explanation of the tasks related to the DRE system interfaces.

Inputs	Outputs
Board of Elections	
• Election Management Software (EMS) is installed on a computer at the Board of Elections (BOE). • The BOE uses the EMS to create the ballot definition that is loaded to the DRE.	
• Workers at the BOE enter data into the DRE to perform the logic and accuracy testing (LAT). • If there is a problem, the BOE troubleshoots the problem and determines if county workers can solve the problem or if the vendor needs to be called.	Workers at the board verify the results that were entered in the LAT.
Vendor	
If there is a problem with the LAT, the vendor may be called in to repair the unit. If the unit is repaired, it must successfully go through the LAT tests before it may be used in an election.	
Poll Workers	
• Poll workers set up the booth. • Poll workers open the DRE for voting. • Poll workers authorize the voter to vote.	Poll workers print a zero tape from the DRE to ensure there are no pre-existing votes recorded on the unit.
Voter	
Voter takes the authorization to vote to the DRE and votes the ballot. The DRE prevents the voter from overvoting, notifies of undervoting, and presents the ballot choices for review as appropriate.	
Poll Workers	
	• Poll workers print result tapes from the DRE. • Poll workers post one result tape at the precinct. • Poll workers remove the media and send the media and a copy of the result tape to the BOE.
Board of Elections	
	• The BOE places the media from the DRE into a media reader, and the EMS tally software counts the votes. • The BOE prints and releases the results.

Work Flow/Process Model

The following diagram provides a graphical overview of the work flow associated with the DRE system interfaces, and represents the next level down from the Context Diagram. This diagram displays the flow of data through the DRE system interfaces in a generic manner. (Refer to each detailed vendor chapter for the process model specific to that vendor.)

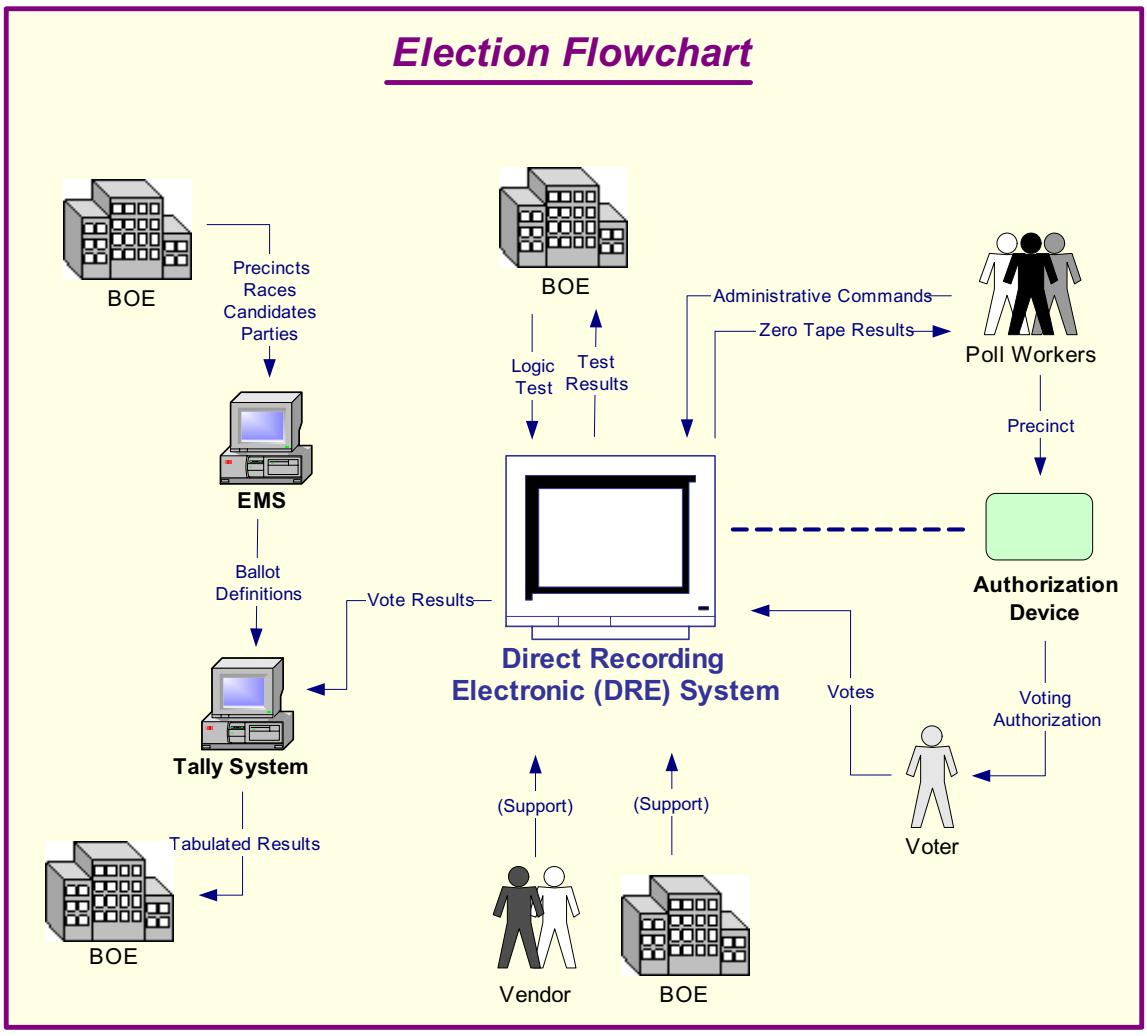

Figure 4 *– Election Flowchart*

Continued on the next page

Work Flow/Process Model (continued)

Following is an explanation of the work flow associated with the DRE system interfaces.

Inputs	Outputs
Board of Elections	
• Election Management Software (EMS) is installed on a computer or on a closed network at the BOE. • Precincts are entered into the EMS either by data entry or by loading from the county voter registration system. • Races are defined in the EMS and related to the precincts. • Candidates are entered into the EMS and related to the races. • The BOE uses the EMS to create the ballot definition that is loaded to the DRE. • A copy of the database is transferred to the Tally software.	
• Workers at the BOE enter data into the DRE to perform the logic and accuracy testing (LAT). • If there is a problem, the BOE troubleshoots the problem and determines if county workers can solve the problem or if the vendor needs to be called.	Workers at the BOE verify the results that were entered in the LAT.
Vendor	
If there is a problem with the LAT, the vendor may be called in to repair the unit. If the unit is repaired, it must successfully go through the LAT tests before it may be used in an election.	
Poll Workers	
• Poll workers set up the booth. • Poll workers open the DRE for voting. • Poll workers authorize the voter to vote.	Poll workers print a zero tape from the DRE to ensure there are no pre-existing votes recorded on the unit.
Voter	
Voter takes the authorization to vote to the DRE and votes the ballot. The DRE prevents the voter from overvoting, notifies of undervoting, and presents the ballot choices for review as appropriate.	
Poll Workers	
	• Poll workers print result tapes from the DRE. • Poll workers post one result tape at the precinct. • Poll workers remove the media and send the media and a copy of the result tape to the BOE.
Board of Elections	
	• The BOE places the media from the DRE into a media reader, and the EMS tally software counts the votes. • The BOE prints and releases the results.

Environment

Hardware Configuration

Following is a summary of the hardware configuration for the four vendors' DRE's.

Processor Type	Processor Clock Speed	Memory	Operating System	Communications Slots	Input Interfaces
Diebold AccuVote-TS					
Hitachi SH3 Family of microprocessors	118 MHz	• 16MB Flash ROM • 32MB RAM - No hard disk • PCMCIA card – 128MB	Windows CE 3.0	• 2 PCMCIA card slots • Smart card reader slot (ISO 7816)	• IrDA • Keyboard • Keypad • Audio • Touch Screen
ES&S iVotronic					
Intel i386 industrial	25 MHz	• 2 MB flash. Includes 3 redundant flash memories. Each are 2 MB. • Flash memory – No hard disk	Proprietary OS and firmware	• 1 (9600 bps) modem • Touchscreen, • 128MB compact flash • PEB (personal electronic ballot) proprietary device with infrared (IrDA) communica-tion	9-pin serial port for null-modem cable access
Hart InterCivic eSlate 3000					
Motorola Coldfire 5307	90 MHz	• 4 MB flash memory. • There are 3 separate memory locations: PCMCIA, eSlate (2 chips), JBC (4 chips) • 128 MB compact flash card – No hard disk	Precise MQX RTOS (real-time operating system) 32-bits	• Stripped down (subset) of RS485, 1MB	Serial RS-485, compact flash

Continued on the next page

Hardware Configuration (continued)

Processor Type	Processor Clock Speed	Memory	Operating System	Communications Slots	Input Interfaces
Sequoia AVC Edge					
National Semiconductor Geode GX1	200 - 333MHz	• 32MB Compact Flash – internal • 64MB DRAM • No hard disk	DOS compatible	• PCMCIA cards/slots	• Serial port on card activator • 2 PCMCIA slots • 1 smart card slot

Software Configuration

Following is a summary of the software configuration for the four vendors' DRE's.

Firmware	User Interface	Internal Storage	Communications Protocols	Security
Diebold AccuVote-TS				
• Operating system is Windows CE 3.0. • Diebold proprietary Firmware is written in 'C'. The voting program itself uses the MFC and is written in C++. • Version evaluated is 2.2.	• Uses a custom GUI interface with simple buttons and a window. • The font is Arial, and there is a minimal amount of graphics.	• No database is used internally to store data. • Data is stored in binary flat files on the PC Card. • Additional fonts and audio are also stored on the Flash Memory.	• Uses TCP/IP over an Ethernet connection. • Uses IDE interface to communicate with removable storage media.	Access is limited by smart card and PIN.

Continued on the next page

Software Configuration (continued)

Firmware	User Interface	Internal Storage	Communications Protocols	Security
ES&S iVotronic				
• The firmware is written in 'C'. • The source is divided into a HAL and the actual voting system.	• Uses a custom GUI interface with simple buttons and a window. • The font is Arial, and there is a minimal amount of graphics.	• No database is used internally to store data. • Data is stored in binary flat files in internal Flash Memory. • Additional fonts and audio are also stored on the Flash Memory.	• No networking is available for an iVotronic. • Uses a proprietary IrDA protocol between a PEB and the iVotronic.	• Machine stays locked until a PEB is inserted. • If a supervisor PEB is inserted, some menus become available. • Some of the supervisor menu functions are blocked by internal passwords.
Hart InterCivic eSlate 3000				
Precise MQX RTOS (real-time operating system) 32-bits	Proprietary GUI software displayed on an LCD allowing user input through push buttons and wheel.	The data is stored in binary format in the PC card in Mobile Ballot Box (MBB), Judge's Booth Controller (JBC) and eSlate devices.	• Stripped down version of RS485, 1MB.	• Voters can access eSlate device using the access code generated by the JBC. • JBC can be set up to have password access.
Sequoia AVC Edge				
DOS compatible	Proprietary GUI software displayed on push button LCD screen.	The data is stored in binary format in the PCMCIA card and AVC Edge internal memory.	Has PCMCIA card slots.	Voters can access AVC Edge device using the smart card, which is activated by the Card Activator.

Requirements Identified

Following is a summary by vendor of the number of requirements tested during Compuware's security assessment.

Note: The number of requirements varied by vendor because the vendors' DRE systems are set up differently, and therefore some requirements did not apply to all of the DRE systems assessed.

Vendor	Number of Requirements Identified	Number of Requirements Not Applicable
Diebold	96	1
ES&S	96	1
Hart InterCivic	96	2
Sequoia	96	1

Note: Administrative policies, procedures, and processes are being tested by InfoSENTRY during their portion of the security assessment.

Test Scenarios

Following is a summary by vendor of the number of test scenarios conducted during Compuware's technical security assessment.

Vendor	Number of Test Scenarios			
	Code Review Tests	Platform Review Tests	Physical Tests	Total
Diebold	30	18	47	95
ES&S	30	18	47	95
Hart InterCivic	30	18	46	94
Sequoia	30	18	47	95

Risks Identified

The results of each test scenario were evaluated and specific risk statements were identified for each vendor. Each risk was analyzed and assigned a likelihood of LOW, MEDIUM, or HIGH. Similarly each risk was assigned an impact of LOW, MEDIUM, or HIGH. An overall risk level was assigned by combining the likelihood with the impact.

Potential Vulnerabilities & Recommended Mitigation Strategies

Compuware has recommended a risk mitigation strategy for each of the risks identified above. These vendor specific mitigation strategies can be found in the Recommended Risk Mitigation Strategy sections of this document for each vendor. The goal of each recommended risk mitigation strategy is to reduce the level of risk to the electronic voting system to an acceptable level.

While conducting the discovery for information on this security assessment a number of general vulnerabilities to the election process were noted. The following mitigation strategies address those general risks and we recommend the SOS implement them in a timely manner in addition to the vendor specific mitigation strategies.

1. **The SOS should implement an Information Technology and Security Policy Standards Document for all related material within any election using a DRE system.**
    a. This point is brought to light since Ohio uses the FEC Standards Document, which is very broad in its security concerns.
    b. The SOS needs to develop a document that would be a formal and concise set of standards for all IT and Software Testing. This document would not be as broad as the Federal Standards and would cover new technology and risks.
    c. The creation of a formal Security Plan would fall in line with a new set of IT and Software Testing Standards for the State of Ohio.

Continued on the next page

Potential Vulnerabilities & Recommended Mitigation Strategies (continued)

2. **The SOS needs to consider the creation of a Security Director position to oversee Policies, Procedures, Information Technology and Security concerns regarding any election in which a DRE system is used.**
    a. This position would require a broad security background ranging from Information Technology, Secure VPN's and LAN-WAN Management to policy and standards creation.
    b. A landline telecommunication background would also be helpful when dealing with remote counties who have limits in their network.
    c. The position's responsibilities would include, but are not limited to, Independent Verification and Validation that the security policies and procedures are followed.

3. **The SOS should consider the implementation of a statewide set of security policies and standards for all counties to follow when using any DRE system.**
    a. One set of security standards and policies should be in place for all counties to adhere to during any election using a DRE system, otherwise there would be inconsistencies in all counties.
    b. If one set of policies is not followed by all, a county not following policy will risk the potential for an unsecured election.
    c. Before any election using a DRE system with any electronic transmission of results is conducted, transmission and auditing requirements need to be defined and implemented.
    d. Security documentation for the entire election process is necessary for election integrity.

4. **After the above three recommendations have been addressed, the SOS will need to consider the creation of a formal Security Training and Awareness Program for all counties.**
    a. To properly implement the new Security Standards and Policies for electronic voting in Ohio, all counties will need to be properly trained.
    b. This will insure that all elections using a DRE system can be secure for both the voter and all of the County Boards of Elections.
    c. If training is not provided to the counties, there is the risk that security controls could be thwarted and the election could be compromised.
    d. A testing or validation process should be implemented which documents that the training was delivered and that the recipient comprehended the essential points of the training.

Continued on the next page

Potential Vulnerabilities & Recommended Mitigation Strategies (continued)

5. **The SOS should require Ohio Voting Machine vendors to demonstrate their software development capabilities by achieving Software Engineering Institute CMM Level 2 certification within one year and achieving CMM Level 3 certification within three years.**
    a. CMM Level 2 ensures the vendor utilizes policies and procedures for managing a software project and has instituted basic software management controls.
    b. CMM Level 3 ensures a standard process for developing and maintaining software is documented and used across the organization. The process integrates both software engineering practices and management processes into a coherent process.
    c. Organizations who have adopted the CMM have reported improvements in productivity and released application quality as a result.

6. **As new versions of DRE software and hardware are released for use in Ohio, the SOS should conduct independent testing similar to this assessment to ensure the voting systems continue to meet all necessary security requirements.**
    a. This process recognizes that each modification to the installed base of voting machines carries the potential to introduce unintended security risks.
    b. Future versions of vendor DRE hardware and software should become more secure as risks are identified and addressed.

The above recommendations apply for a DRE System that is not connected to a network. If the systems being used were to be connected to a network for possible voter identification, elections results or election setup, the recommendations above would need to be amended. Since there is a possibility for the County Boards of Elections to connect DRE's to a network in the future, it is recommended that all possible network security issues be included in any future document.

Currently the SOS and County Boards of Elections have no formal Information Technology, Software or Security Standards and Policies Guidelines with regard to DRE systems. If the County Boards of Elections proceed with an election without using the above recommendations, they have a high risk of vulnerabilities. These vulnerabilities could result in election tampering and fraud when using a DRE System.

Conclusion

Compuware conducted a study of four DRE voting systems from vendors who were qualified by the state of Ohio to help upgrade the state's voting systems as required by HAVA. Our study identified specific security vulnerabilities that might be exploited during an election and recommends actions to mitigate these vulnerabilities. The scope of this study was limited to reviewing the technical implementation of each DRE plus reviewing each data stream into and from the DREs. It did not include a review of the policies, procedures, or work practices of either the vendors or the Ohio Secretary of State.

During the course of our study, Compuware identified several significant security issues, which left unmitigated would provide an opportunity for an attacker to disrupt the election process or throw the election results into question. These are documented throughout this assessment report. Following careful consideration of each of these security issues, we developed mitigation recommendations for the Secretary of State to implement which we believe will limit the likelihood of a successful attack or inadvertent disruption to the election process. Provided that mitigating strategies are executed for each risk identified before the systems are used in an election, Compuware concluded that the Secretary of State can securely deploy these voting machines.

Election policies and procedures have long been used to ensure fair and accurate election results. The deployment of electronic voting technology will not lessen the need for well thought out and consistently enforced policies and procedures.

PART TWO: DIEBOLD

Overview

This section details the assessment for the Diebold AccuVote-TS DRE. The AccuVote-TS system is a voter-activated interactive touch-screen system.. Using a smart card as the voter authorization, the AccuVote-TS permit voters to view and cast their votes by touching target areas on an electronically generated ballot.

Each unit provides a direct-entry computerized voting application that automatically records and stores appropriate ballot information and results. At the end of the voting period, the system can print precinct totals to be included as part of the permanent record.

The AccuVote-TS is supported by the Global Election Management System (GEMS) software, which provides ballot creation, vote tabulation, and reporting.

The AccuVote-TS prevents the voter from overvoting, notifies the voter of undervoting, and allows the voter to review and modify their ballot choices before casting their ballot.

Compuware tested the following hardware and software in this technical security assessment:

Hardware	Software
• AccuVote-TS R6, Firmware version 4.3.15 • Voter Card Encoder version 1.1.4	Global Election Management System (GEMS) version 1.18.18

Step 1: Characterization of the AccuVote-TS Voting System

In Step 1, the AccuVote-TS was examined for the following:

- AccuVote-TS system interfaces – input/output connections between the AccuVote-TS and external entities, and the related voting processes
- Work flow / process model – flow of data through the AccuVote-TS system interfaces, and the related voting processes
- AccuVote-TS environment
  - Hardware configuration
  - Software configuration
  - Network configuration

AccuVote-TS System Interfaces

The following diagram provides a graphical overview of the connections to the AccuVote-TS. The diagram shows the input/output connections between the AccuVote-TS and external entities such as the BOE's and voters.

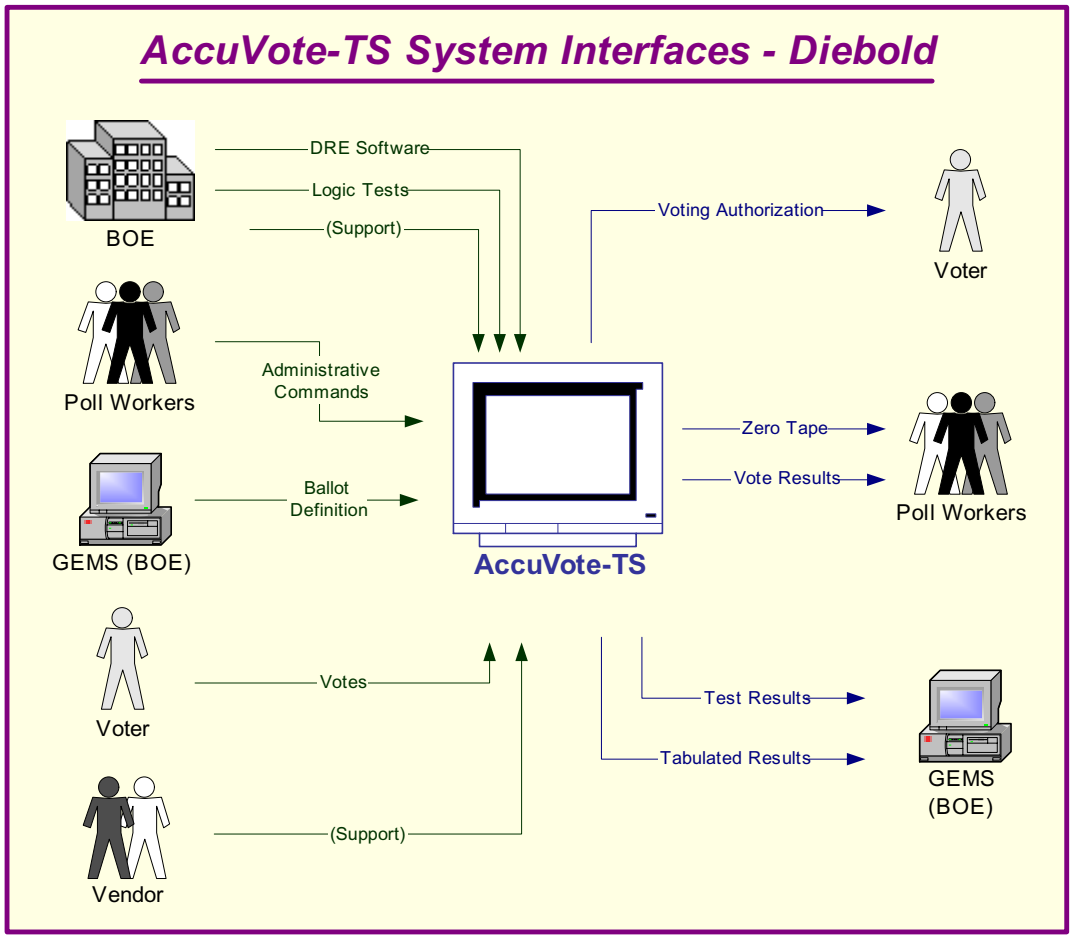

Figure 5 – *AccuVote-TS System Interfaces - Diebold*

Continued on the next page

AccuVote-TS System Interfaces (continued)

Following is an explanation of the tasks related to the AccuVote-TS system interfaces.

Inputs	Outputs
Board of Elections	
• Global Election Management Software (GEMS) is installed on a computer at the Board of Elections (BOE). • The BOE uses the GEMS to create the ballot definition that is loaded onto the AccuVote-TS.	
• Workers at the BOE enter data into the AccuVote-TS to perform the logic and accuracy testing (LAT). • If there is a problem, the BOE troubleshoots the problem and determines if county workers can solve the problem or if the vendor needs to be called.	Workers at the board verify the results that were entered in the LAT.
Vendor	
If there is a problem with the LAT, the vendor may be called in to repair the unit. If the unit is repaired, it must successfully go through the LAT before it may be used in an election.	
Poll Workers	
• Poll workers set up the booth. • Poll workers open the AccuVote-TS for voting. • Poll workers authorize the voter to vote by issuing the voter a smart card.	Poll workers print a zero tape from the AccuVote-TS to ensure there are no pre-existing votes recorded on the unit.
Voter	
• Voter receives the smart card and inserts it into the AccuVote-TS, which presents the correct ballot for the voter. • Voter votes the ballot. The AccuVote-TS prevents the voter from overvoting, notifies of undervoting, and presents the ballot choices for review as appropriate.	
Poll Workers	
Poll worker receives the smart card from the voter after the voter casts the ballot.	• Poll workers print result tapes from the AccuVote-TS. • Poll workers post one result tape at the precinct. • Poll workers remove the media and send the media and a copy of the result tape to the BOE.
Board of Elections	
	• The BOE places the media from the AccuVote-TS into a media reader, and the votes are counted by the GEMS tally software. • The BOE prints and releases the results.

Work Flow / Process Model

The following diagram provides a graphical overview of the work flow associated with the AccuVote-TS system interfaces, and represents the next level down from the Context Diagram. This diagram displays the flow of data through the AccuVote-TS system interfaces.

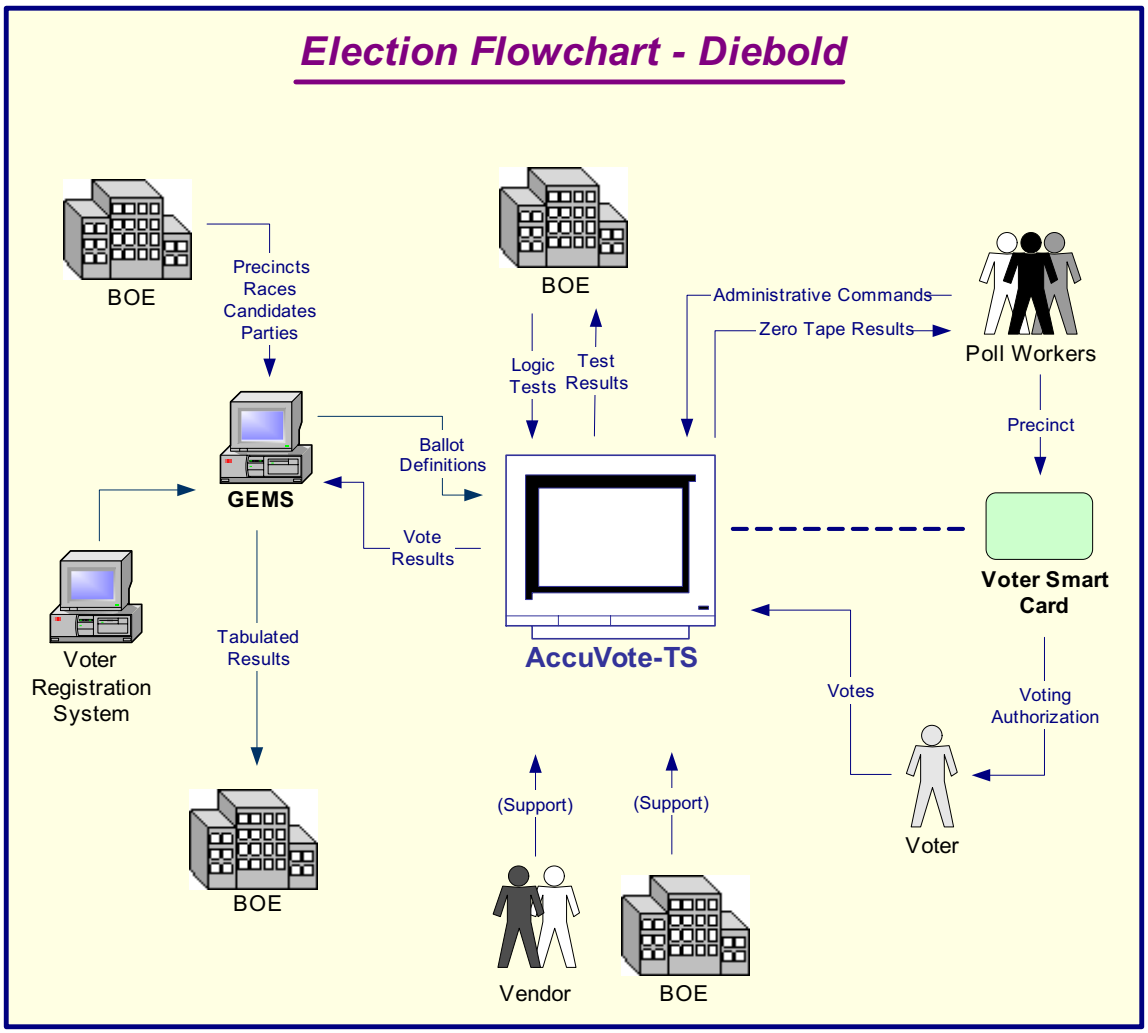

Figure 6 *– Election Flowchart - Diebold*

Continued on the next page

Work Flow/Process Model (continued)

Following is an explanation of the work flow associated with the AccuVote-TS system interfaces.

Inputs	Outputs
Board of Elections	
• Global Election Management Software (GEMS) is installed on a computer or on a closed network at the BOE. • Precincts are entered into the GEMS either by data entry or by loading from the county voter registration system. • Races are defined in the GEMS and related to the precincts. • Candidates are entered into the GEMS and related to the races. • The BOE uses the GEMS to create the ballot definition that is loaded to the AccuVote-TS.	
• The PCMCIA card that contains the ballots is inserted into the AccuVote-TS. • Workers at the BOE enter data into the AccuVote-TS to perform the logic and accuracy testing (LAT). • If there are problems, the BOE troubleshoots the problem and determines if county workers can solve the problem or if the vendor needs to be called.	Using the GEMS Tally feature, workers at the BOE verify the results that were entered in the LAT.
Vendor	
If there is a problem with the LAT, the vendor may be called in to repair the unit. If the unit is repaired, it must successfully go through the LAT before it may be used in an election.	
Poll Workers	
• Poll workers set up the AccuVote-TS voting booth. • Poll workers open the AccuVote-TS for voting. • Poll workers authorize the voter to vote by issuing the voter a smart card.	Poll workers print a zero tape from the AccuVote-TS to ensure there are no pre-existing votes recorded on the unit.
Voter	
• Voter receives the smart card and inserts it into the AccuVote-TS, which presents the correct ballot for the voter. • Voter votes the ballot. The AccuVote-TS prevents the voter from overvoting, notifies of undervoting, and presents the ballot choices for review as appropriate.	

Continued on the next page

Work Flow/Process Model (continued)

Inputs	Outputs
Poll Workers	
Poll worker receives the smart card from the voter after the voter casts the ballot.	• Poll workers print result tapes from the AccuVote-TS. • Poll workers post one result tape at the precinct. • Poll workers remove the PCMCIA card and send the card and a copy of the result tape to the BOE.
Board of Elections	
	• BOE places PCMCIA card from the AccuVote-TS into an AccuVote-TS that is serving as a media reader, and the GEMS tally software counts the votes. • The BOE prints and releases the results.

Environment

Hardware Configuration

Following is a summary of the hardware configuration of the Diebold AccuVote-TS that was tested.

Processor Type	Processor Clock Speed	Memory	Operating System	Communications Slots	Input Interfaces
Hitachi SH3 Family of microprocessors	118 MHz	• 16MB Flash ROM • 32MB RAM - No hard disk • PCMCIA card – 128MB	Windows CE 3.0	• 2 PCMCIA card slots • Smart card reader slot (ISO 7816)	• IrDA • Keyboard • Keypad • Audio • Touch Screen

Software Configuration

Following is a summary of the software configuration of the Diebold AccuVote-TS that was tested.

Firmware	User Interface	Internal Storage	Communications Protocols	Security
• Operating system is Windows CE 3.0. • Diebold proprietary Firmware is written in 'C'. • Version evaluated is 2.2.	• Uses a custom GUI interface with simple buttons and a window. • The font is Arial, and there is a minimal amount of graphics.	• No database is used internally to store data. • Data is stored in binary flat files on the PCMCIA Card. • Additional fonts and audio are also stored on the Flash Memory.	• Uses TCP/IP over an Ethernet connection. • Uses IDE interface to communicate with removable storage media.	Access is limited by smart card and PIN.

Environment (continued)

Network Configuration

There is a network-based LAN/WAN port intended for communication of ballot definitions and voting results between the AccuVote-TS and the GEMS election management software. The network functionality is provided by a removable PCMCIA network card using standard TCP/IP protocol over an Ethernet connection. Diebold has limited their firmware to only recognize a small number of PCMCIA network cards. This networking capability should be removed from the AccuVote-TS during balloting. A locking door covers the port where the PCMCIA modem is installed during the election process.

Step 2: Threat Identification

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. Vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised. In determining the likelihood of a threat, one must consider threat-sources, potential vulnerabilities (Step 3), and existing controls (Step 4).

In Step 2, the assessment team determined the potential threats posed to the AccuVote-TS voting system. Following is a list of potential threats to which the AccuVote-TS voting system could be exposed.

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Campaign and political entities	Competitive advantage Economic espionage Change outcome of election	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Step 3: Vulnerability Identification

The analysis of the threat to an electronic voting system must include an analysis of the vulnerabilities associated with the system environment. In Step 3, the assessment team identified vulnerabilities (flaws or weaknesses) of the system. Results from audits, tests, inspections, and an examination of the current state of the AccuVote-TS voting system were used to determine existing weaknesses.

The assessment team conducted a comprehensive review of compliance to both technical and non-technical requirements to identify vulnerabilities. In addition to identifying weaknesses in the above, the team also assessed external entities and their connectivity to the AccuVote-TS voting system.

Requirements Tested & Test Results

This section documents the requirements that were tested, the tests conducted, and the results of each test.

Test Areas

Tests were conducted in the following areas.

1. Code Review Tests
2. Platform Review Tests
3. Physical Tests

Specific Tests and Test Results

The assessment team tested the specific scenarios listed below. For each scenario, the table lists:

- Description of the requirement tested
- Test Scenario that covered the requirement
- Test Results

No.	Requirement	Test Scenario	Test Results
Code Review			
Standardization - Naming conventions of variables, constants and modules should be consistent across the application. Construction of modules within an application should also be consistent. This is important for knowledge transfer and code maintenance.			
1.01	There shall be a standard method in the naming of functions and variables.	Perform visual review of source files. Function names will be checked for proper case formatting of concatenated words. Names of functions should clearly describe its purpose.	There is a standard for the naming of the code. The naming conventions of the variables and constants across modules are consistent and clear using good coding standards.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
1.02	There shall be a standard method in the construction of modules.	Perform visual review of source files. Modules should contain a consistent format and location for module components. Modules should begin with comments describing the modules contents. Location of methods and variables with associated comments should be consistent throughout.	The modules contain descriptive file names, and descriptions of the tasks performed. The modules appear consistent file to file.
Coding Conventions - The application should be broken down into modules with each module performing a single function. There should be single entry and exit points within a module. There should be consistent error handling throughout the application. Naming of variables, constants and modules should be descriptive and self-explanatory.			
1.03	There shall be a standard methodology used for the construction of modules.	Perform visual review of source code. Modules should use a clear methodology of construction. Files will be reviewed to see if a coding industry standard is used in the naming of modules, functions, variables and constants.	The construction of the modules is consistent across all files. Components of each modules are easy to identify. In the software specifications it mentions a preference to follow the K&R style and Hungarian notation as well. These formats are closely followed in the source code.
1.04	The naming of variables and functions shall be clear and descriptive.	Perform visual review of source code. Function and variable names should be "self documenting" as well as contain properly typed and sized attributes, and return types.	Variables are well named and are clearly used throughout the source code. There is appropriate use of single letter variables in loops.
1.05	There shall be a consistent way to handle system errors.	Perform visual review of source code for implementation of error handling code. All methods should contain error-handling logic. Systems should remain stable in the event of an error. When an error occurs, sufficient information regarding the state of the system and system parameters should be recorded for future debugging.	The system is written in Visual C++ using Microsoft Foundation Classes. This environment provides C++ statements and MFC classes for error and exception handling. These include the **try**, **catch**, and **throw** statements of Visual C++. Blocks are provided in the software, using these features, to detect and respond to exception and error conditions. If, during system operations, an error or exception condition is detected, either by the system or by some library function, an Exception is thrown. This Exception will then be caught by the first catch block that matches the Exception.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
Code Documentation - All source code should be sufficiently commented, with clear descriptions of what is being accomplished by each module, the names of calling functions, and the inputs and outputs to the modules. Consistency should be maintained in commenting the code for ease of readability.			
1.06	The comments in the code shall be descriptive and present in the code.	Perform visual review of source code. Comments will be reviewed for simple descriptive content. Comments should appear at the beginning of each module, function. All module level variables, constants, and structures should be commented as well. Function parameters and return values should describe appropriate values. Comments should also appear in methods to help clarify complex code and logic behind expressions.	Comments do appear at the top of all source modules. Module variables are individually commented or for functional areas. Functions are commented but parameters and return values are, in most instances, not commented. For long and complex methods there are comments helping to clarify long code segments.
1.07	The comments shall have a consistent look in their layout.	Perform visual review of source code. Comments should have a common format with standard fields for information. Some standard fields should be a description, parameters, return types, a change log.	There is a consistent use of comments through out the code for identifying the functionality of methods. There are descriptions for almost all methods, but additional comments for parameters and return values is not available
1.08	The modules shall be commented describing their contents.	Perform visual review of source code. Modules should have a standard comment identifier at the beginning of each module. Module comments should contain the name and description of the module, a copyright notice, and a change log.	There are comments that begin each module. The comments include the name of the file, the revision history, and a detailed description of the functionality contained in the module.
1.09	There shall be a close relationship of the requirements to the code modules that implement the requirements.	Perform visual review of the source code. Modules will be reviewed for their functional content. The variables and functions should be closely related and work directly to perform a clear task.	In reviewing the code modules and the provided software requirements, a close relationship was not found between the source code and the written requirements.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
Coding Complexity - Code should be simple in construction. It should be easy to read and follow. Modules should perform single tasks and should have single points of entry and exit.			
1.10	The system shall be divided into modules.	The source code will be visually reviewed to verify if the code has been properly modularized. Modules should be an appropriate length and encapsulate related functionality.	The source code has been broken into functional areas and then further broken down into individual source modules. Though some modules are long, their size is appropriate.
1.11	The source code shall use simple logic structures.	The source code will be visually reviewed for the use of simple and clear logical structures. There should be the use of constants (consts) and data structures (structs) to improve code readability and reliability.	The source code does have a lot of use of simple data structure constructs. When a construct is used the internal components are clear and closely related. Variables are passes around by reference for efficiency in memory usage and system speed.
1.12	The source code shall have an appropriate size of modules and the number of functions performed by them.	The source code will be visually reviewed to verify if the code has been properly modularized. Modules should encapsulate related functionality into logical groupings with clear interfaces. Interfaces should be well defined as to their use.	Some of the modules are quite large but they appear to be limited to critical areas of functionality where considerable processing is required. The functionality of modules is well grouped. They are well laid out and easy to follow.
Classes / Modules - Use of classes / modules can make the code smaller and reusable.			
1.13	There shall be the existence of classes and modules.	The source code will be visually reviewed to verify implementation of classes and proper modularization of the source files.	The modularization of the source code appears to be well thought out and appropriate. The groupings of functional elements are clear and well reasoned. Where there are questions as to where to put a component, there are comments describing the quandary and the reasoning behind the decision.
1.14	The functions performed by the classes shall be self-contained where appropriate.	The source code will be visually reviewed. The name and description of the class should be simple and clear. The task performed by the function should be easy to understand, simple to define, and atomic.	The C++ source code has an appropriate use of encapsulation and interfaces. The use of access qualifiers is appropriate to make class interfaces clear, and to understand how to use the modules.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
Third Party Components - Use of third party components requires strict guidelines, security standards and version control. Attention will be paid to controls around third party components used in the applications.			
1.15	Any use of third party components in the firmware shall be inspected.	The source code will be visually reviewed to find any use of third party products. The makers and the versions of any found third party applications will be noted.	There is use of several third party components. Audio playback is from an open source library named Fmod. The version used is not known. Access of the external flash memory is from FlashFx from the Datalight Corporation. Both of these are used as packages and the source code was not available.
1.16	Any third party components shall be secure and not create a risk.	If the source is available for any used third party products, the source will be reviewed for client modifications. Third party source code should only contain the necessary functionality with unused areas removed or disabled. If the source is not available then further study will be required.	Diebold does not maintain the third party packages. Updates come from the owner of the source code. In the case of Fmod, it is an open source package where the source code is freely available to anyone. **Note:** In order to exploit a vulnerability it would require the attacker to be able to create, compile and include malicious files on the AccuVote-TS when the firmware is upgraded.
Database Review - Database integrity and data security is vital for correct data reporting. The code review will include the following:			
1.17	The database shall be well designed.	The data model and database source code will be reviewed for existence of proper keys and normalization.	There is no use of a database on the AccuVote-TS. Data files are stored in internal and external memory as binary flat files.
1.18	The data in the database shall be secure.	The source code will be visually reviewed for user access levels and roles implemented as part of security.	Not applicable to the design of the Diebold AccuVote-TS.
Data Integrity - Review the internal data storage of the system using the following criteria:			
1.19	There shall be ways to verify the correctness of system data.	Source code will be reviewed and tested in order to check for CRC techniques in verifying the correctness of data that is stored in memory. Can the software identify data that has been improperly modified?	The contents of the memory are check summed. The type of checksum is a CRC16 format. The data is verified at the time the ballots are first loaded and after every vote.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
1.20	There shall not be any means by which a voter can be identified.	The source code will be reviewed to make sure that an algorithm is implemented to make sure voter records are stored in random order. The Cast Vote Records should not have time stamp associated with it.	The votes are stored in a random order into separate vote buckets. The vote records are hashed in a random order to prevent determination of the vote order.
1.21	The system shall be secure and prevent any access other than from authorized voters or supervisors.	The source code will be reviewed to verify the system is secure and allows each voter to only vote once by issuing unique access codes.	A voter card controls voter access. The voter card is a smart card issued only from Deibold. Voter cards are activated by using a card reader to properly identify the precinct of the voter. The information on the voter card only allows the DRE to identify and present the proper ballot for the voter. Immediately after voting the card is disabled and ejected from the DRE and the voter is to return the card to the poll workers. The supervisor's access is limited with a Supervisor's card and a PIN must be entered. The PIN is set by Diebold and is the same for all DREs of this type.
1.22	There shall be a system to protect and back up data in the event of a disaster.	The source code will be reviewed to verify there is a means by which votes can be recovered in case of a system disaster.	All results are stored on the removable flash memory. Additionally the results are stored on an internal flash memory that can be removed if needed.
Encryption Standards - Review of encryption standards used in the DREs and the supporting software will be a point of primary focus while the source code is being reviewed.			
1.23	There shall be a strong method of encryption used.	The strength of encryption will be reviewed. The types of encryption will be reviewed to see if it is sufficient.	Diebold stores ballot definitions and Cast Vote Records on the PCMCIA removable media. The Cast Vote Records are encrypted with a DES encryption package.
1.24	The data shall be encrypted including "*ballot definitions*" and other data on the DREs.	Ballot Definitions and Cast Vote Records should be protected and be verifiable they are correct. Encryption should be powerful enough to block access to stored data.	Diebold stores ballot definitions and Cast Vote Records on the PCMCIA removable media. The contents of the data are encrypted with a DES encryption package.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
1.25	There shall be the use of cryptographic operations during voter authorization.	Various means of "voter identification" should be secure. The data on a voter authorization token should not be discernable.	Voter Smart cards are used to allow access to a AccuVote-TS. The contents of the voter card are not encrypted but access is limited by internal hardware keys that are specific to the system. These keys prevented direct access to the contents of the smart card.
1.26	There shall be the use of encryption keys protecting types of removable media. Those keys shall be protected during the transportation of Ballot Definitions and Voting Records.	Encryption keys should be randomly generated every time and sufficiently long so that it is not easy to guess. The key its self should be kept private and not easily discovered.	The Diebold Accuvote-TS does use a DES type of encryption. The key for the encryption is currently hard coded in the system.
1.27	Any data transmitted shall be encrypted over communication links.	Transmission protocols will be checked for the use on encryption. Data should never travel over a wire without protection. The contents of the transmission should be verifiable as to their contents and correctness. Any type of tampering should be identifiable if not impossible.	Data is not encrypted when transmitted over a data link.
1.28	The AccuVote-TS shall not have unencrypted cast ballot records.	Check the vote records on the AccuVote-TS, GEMS software, and transfer medium to ensure that the records are encrypted.	Contents of the voting records are encrypted using DES.
1.29	The AccuVote-TS shall not have unencrypted audit logs.	Check the audit logs on the AccuVote-TS to ensure that they are encrypted.	Contents of the audit logs are encrypted using DES.
1.30	The system shall not store or use passwords without encryption.	Perform code review to ensure that passwords used in all software are encrypted.	There are no passwords that are stored. There is a hard coded system access in the source code.
1.31	The system shall not use hardcoded passwords.	Perform code review to ensure that the system does not use hardcoded passwords.	The only password is the supervisor's password and it is hard coded.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
Platform Review			
2.01	The AccuVote-TS shall not allow supervisor privileges to unauthorized individuals.	Attempt to convert a valid Voter smart card into a Supervisor smart card that is recognized by the AccuVote-TS.	We were unable to manufacture a counterfeit Voter smart card or to convert a Voter smart card into a Supervisor Card. Using an ACR80 Card Tool purchased on-line we were able to read and write to the EEPROM on both the Voter and Supervisor cards. We changed the default string in the EEPROM from ?@ABCDEF to TacoTest and could then read the value 'TacoTest' back. This was also the case with a valid Voter card with Precinct.001 ballot on it. The EEPROM was able to be read as well as write the value 'TacoTest' to it. We were able to use the ACOS card player to issue the following commands with successful execution: Start Session, Authenticate, Submit Code, Select File, and Change PIN on both the Voter card and the Supervisor card. These commands completed successfully but the files, records, and code submitted as commands did not return any relevant data even though the commands completed successfully. WE also were able to setup Encryption/Decryption on both cards with the ACR80 Card Tool. We tried to create a counterfeit voter card out of a blank ACS smart card on the AccuVote-TS. The response was: Please remove the Voter Card and try again or press Cancel to abort. Finally we tried to create a Voter Card out of a third party card and the response was: Card upside down or not inserted correctly. Please remove the Voter Card and try again or press Cancel to abort.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
2.02	The system shall not allow unauthorized modification of the Ballot Definition file.	Try to modify the Ballot Definition file on the PCMCIA card before loading it on the AccuVote-TS. Try to modify the card using a simple laptop and then insert it in the AccuVote-TS.	File would not load from the PCMCIA card. The system warned of a bad file and would not load the files from the card. The AccuVote-TS recognized that the files were changed on something other than the AccuVote-TS or voting software.
2.03	The AccuVote-TS shall not allow the installation and/or execution of an unauthorized program.	Install a program on a PCMCIA card, insert it in the AccuVote-TS, and install and/or execute the unauthorized program.	The system would not load an executable file by itself, and attempts to use the Win CE to find the file on the PCMCIA card were unsuccessful.
2.04	The system shall not allow for security breaches via the internet.	Inspect the AccuVote-TS for network accessible ports.	The AccuVote-TS connects to the network through a PCMCIA network card with Windows CE TCP/IP protocols. This is the normal port for loading ballot definitions and uploading cast ballot records.
2.05	The system shall not allow for security breaches via the internet.	Try to access, modify, or disrupt the functioning of the AccuVote-TS software while connected to a network.	A laptop computer was connected to the network with an AccuVote-TS and GEMS server. Several attempts were made to gain control of or modify information on the AccuVote-TS from the laptop. None of these attempts were successful at accessing the information within the AccuVote-TS.
2.06	The AccuVote-TS shall be resistant to tampering, lock up, intrusion or vandalism.	Try to bring the system down, lock up the operating system, change or erase log files, or any other form of Denial of Service (DoS), Distributed Denial of Service (DDos), or other result which benefits the attacker.	The system has a lock and key in place to covered ports and system reset. Could not tamper with system while lock cover in place and keyboard attached. If the cover is open, the operating system and/or the application, BallotStation.exe, can be locked up by pressing the function key F4 which brings up the Open File dialog box. By navigating to \FFX\Bin and invoking BallotStation.exe the system locks up or freezes.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
2.07	The AccuVote-TS shall not allow supervisor privileges to unauthorized individuals	Tests were preformed to change a voter smart card to supervisor card. We were able to read and write to the Diebold card but we could not change the voter card to a valid supervisor card with a smart card reader and writer.	We were unable to counterfeit a Voter smart card or convert a Voter smart card into a Supervisor Card with the equipment we had available. This does not prove a working smart card cannot be counterfeited but does indicate it is not an easy task to accomplish. There is a risk that an unauthorized person might be able to create and use a counterfeit smart card to access supervisory functions or cast extra ballots.
2.08	The operating system on the AccuVote-TS shall be hardened against unintended intrusion, operations, or forced errors.	Try to cause a kernel panic, system failure, or indefinite wait state, or other operating system lock-up within the operating system or sub-system. With the access panel open and a keyboard or keypad plugged in, multiple or simultaneous keystrokes hit or key combinations pressed simultaneously was the main method of attack.	No attempts could be made while the cover was locked. When the cover was open, ports were available but we were unable to produce any kernel panics, wait states, or other operating system lock-ups, freezes, or general protection faults or invalid page faults in the AccuVote-TS.
2.09	The system shall password protect supervisor functions.	Observe that functions are password protected, the minimum length of passwords, and that they can be changed.	The password or PIN used for the supervisor smart card is the same for all cards by Diebold. It is a four-digit number and was guessed on the third attempt, and we gained access to the supervisor functions on the AccuVote-TS. The four-digit PIN is a factory default from Diebold and cannot be changed.
2.10	The system shall not allow corruption of the O/S, application program, ballot definition, or voter data.	Try to create an attack on flash memory using files loaded on the PCMCIA card.	File would not load from the PCMCIA card. The system warned of a bad file and would not load the files from the card. The AccuVote-TS recognized that the files were changed on something other than the AccuVote-TS or voting software.
2.11	The system shall not allow undetected tampering with or modification to the contents of removable media.	Change the contents on a removable media card and use the card. Determine if the system reports the card has been modified.	When the clear text parts of a binary file were changed, the system recognized it as a bad file and would not load it onto the AccuVote-TS.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
2.12	The AccuVote-TS shall maintain a protective counter of the total number of votes cast in all elections.	Try to modify protective counter.	There was no way to access the protective counter through ports, PCMCIA card or Supervisor smart card via telnet, FTP, voter card changes, or additions to the PCMCIA card to change the protective counter.
2.13	The AccuVote-TS shall not allow "Man-in-the-middle" attacks when communicating between the Election Management Software and the AccuVote-TS.	Examine the hardware and communication architecture to determine if TCP hijacking attacks are possible.	The AccuVote-TS is not on a network and uses a direct connection to the management software within a few feet.
2.14	The AccuVote-TS shall protect all COM ports from intrusions or vulnerabilities.	Try to gain access via an open TCP/UDP or serial or USB or other port.	An Nmap scan revealed the following ports/services were filtered: 21/tcp-ftp, 389/tcp-ldap, 1720/tcp-H.323/Q.931 (where H.323 is the teleconferencing protocol for voice/data/video IP telephony). Filtered ports are usually covered by a firewall, filter or other device. The following ports are also open (where an open port is defined as "will accept connections on that port"): 21/tcp-ftp, 25/tcp-smtp, 110/tcp-pop3, 389/tcp-ldap, 1002/tcp-unknown, 1720/tcp-H.323/Q.931 (Q.931 is a ISDN connection control protocol).
2.15	The AccuVote-TS shall be resistant to introduction of Trojans, viruses, or any other form of malware.	Try to introduce any type of malicious software (malware) into the system.	Putting a program on a PCMCIA card did not work since the system would not load it. Attempts to load a program through an open port were unsuccessful.
2.16	The system shall have a programmable memory device that is sealed in the unit with means of tamper detection.	Inspect the hardware design documents and physical hardware.	The system was sealed shut with no access to the flash memory. When the PCMCIA card slot is locked, there is no way to access it without the key.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
2.17	The system shall provide for safeguards against and evidence of tampering, theft or damage of the system and units.	Inspect the physical hardware for location of seals and locks and for safeguards against and evidence of tampering.	The unit provides for an external lock and/or seal which would prevent undetected tampering, provided duplicate seals were not available.
2.18	In the event of the failure of a unit, the system shall retain a record of all votes cast prior to the failure	Voted on unit, then removed power. The unit was left on overnight to drain the battery. The unit was started back up and checked for correct data.	When power was pulled or drained the memory was kept on the flash. No voting data was lost or corrupted.
Physical Testing			
3.01	There shall be a programmable memory device sealed in unit with means of tamper detection.	Check PCMCIA card to determine whether it can be removed easily and can be locked.	The PCMCIA card is housed in a lockable compartment and it cannot be removed when locked.
3.02	Poll opening reports should have all system audit information required	Conduct logic and accuracy tests and verify system audit information is present.	Accuracy and logic tests were conducted before the election. System audit information is displayed on the resulting print out.
3.03	The system shall store logic and accuracy test results in memory of the main unit processor and Election Day device	Conduct logic and accuracy test and verify results are recorded in the on-board memory by printing the audit log.	Accuracy and logic tests were conducted before the election to verify system information was correct. Logic and accuracy test result were printed in the audit log.
3.04	The system shall provide logic and accuracy tests in the memory of the main processor and the programmable memory device used on Election Day, including zero printouts before each election and a precinct tally printout at the close of each election	Conduct logic and accuracy testing before election is started. Print a zero tape before an election and a result tape after an election.	Accuracy and logic tests were conducted before the election to verify counters are working properly and the programming for each voting device is correct. A zero tape printout was created and verified that no votes were cast before the start of the election. After voting was closed, a result tape was printed.
3.05	The system shall control logic and data processing methods to detect errors and provide correction method.	Create an instance where a known error will occur on the AccuVote-TS. For instance, enter a voter card after it has been de-activated.	AccuVote-TS displays a concise error message. This is standard throughout all error handling functions on the AccuVote-TS.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.06	The AccuVote-TS shall provide a mechanism for executing test procedures which validate the correctness of election programming for each voting device and polling place and insure that the ballot display corresponds with the installed election program.	Conduct a logic and accuracy test.	Accuracy and logic tests were conducted before the election to verify counters are working properly and the programming for each voting device is correct.
3.07	The EMS software shall not allow unauthorized modification of the Ballot Definition data.	Try to modify the Ballot Definition in the GEMS software using a database viewer/program.	We were capable of viewing the ballot definition file through Microsoft Access. Changes could be made to the database and all records can be viewed. The audit log is also stored in the database and could be viewed and edited.
3.08	The system shall present the ballot to the voter in a clear and unambiguous manner.	Create an election ballot definition file and transfer the file to the AccuVote-TS. Open election and look at ballot.	The ballot is presented in a clear and unambiguous manner.
3.09	The AccuVote-TS shall not allow voters to vote multiple times.	Insert a counterfeit smart card into the AccuVote-TS and try to use it to vote.	Unable to produce a working counterfeit smart card.
3.10	The AccuVote-TS shall not allow voters to vote multiple times.	Insert an authorized smart card into the AccuVote-TS and try to use it to vote multiple times.	Once a vote has been cast, the smart card used is deactivated. When trying to insert the deactivated smart card to vote again, the card is ejected from the reader.
3.11	The system shall not allow voting access to unauthorized persons.	Create a counterfeit Voter Access smart card then attempt to use it so it is recognized and authenticated by the AccuVote-TS.	Unable to produce a working counterfeit smart card.
3.12	The AccuVote-TS shall not allow viewing or changing vote results during the election process.	Insert a supervisor card in the AccuVote-TS and try to view or change vote results.	The supervisor menu does not allow a user to change or view vote results. Results can only be viewed and/or printed after election has been closed.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.13	The AccuVote-TS shall not allow the accidental or unauthorized closing of the election.	Insert a Supervisor Card in the AccuVote-TS and try to terminate the election early.	With the use of a supervisor card and the correct PIN number, we were able to close the election early. Inserted the supervisor card, entered the four-digit pin, and the AccuVote-TS prompted, "Do you want to close the polls? Yes/No".
3.14	The AccuVote-TS shall not allow the accidental or unauthorized reset of the AccuVote-TS.	Insert a Supervisor card in the AccuVote-TS and try to reset the AccuVote-TS.	The AccuVote-TS cannot be reset during voting. Once voting is closed, the AccuVote-TS can be reset with a supervisor card and the correct PIN number. Resetting clears the memory on the AccuVote-TS and can clear the PCMCIA card as well.
3.15	The AccuVote-TS shall not allow the use of an unauthorized PIN to access supervisor functions.	Insert an authorized supervisor card in the AccuVote-TS and try to access supervisor functions using an incorrect PIN.	User is denied access when using an incorrect PIN. An error message is clearly displayed to the user. The supervisor PIN number is the same for all supervisor cards distributed by Diebold and was guessed in three tries during our testing.
3.16	The AccuVote-TS shall not lose voter information, vote count, Ballot Definition information, etc. due to a power outage during the election.	Start voting on the AccuVote-TS, and then disconnect batteries/power for 30 minutes to simulate a power outage, Resume power and start up the AccuVote-TS, and check the voter information.	Removed power cord and AccuVote-TS voting machine has a battery backup that powered the machine. The battery is sealed within the machine and could not be removed.
3.17	The AccuVote-TS shall not lose voter information, vote count, Ballot Definition information, etc. due to a power outage during the election.	Start voting on the AccuVote-TS, and then disconnect power for thirty minutes to simulate a power outage, and then resume power. Cast votes before, during, and after the disruption.	Removed power cord and AccuVote-TS voting machine has a battery backup that powered the machine. The battery is sealed within the machine and could not be removed.
3.18	The AccuVote-TS shall not allow for modification of the "protective counter" which tracks the total number of votes cast on the machine.	Try to modify the protective counter on the AccuVote-TS.	Supervisor functions will not allow the altering of counts on the AccuVote-TS voting machine. Counter is stored within the CPU on the AccuVote-TS. The number on the counter is printed out before the election and after the election as well.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.19	The AccuVote-TS shall not allow modification that forces it to use the same storage device for all of the data.	Modify the AccuVote-TS so that only core flash memory is available and see if the system will allow voting.	User is prompted to turn off machine or insert memory card. The system will not allow only one memory source.
3.20	The system shall not allow supervisor access to unauthorized persons.	Try to convert a Voter Access card to a Supervisor card then access and perform supervisor functions in the AccuVote-TS.	Unable to convert a Voter Access card to a Supervisor card.
3.21	The audit logs shall record all instances of supervisor access to the AccuVote-TS.	Review audit log after completing successful vote test and ensure each step that used supervisor access is correctly logged.	Each time a supervisor card is used, the action is logged within the audit logs specific to the AccuVote-TS.
3.22	The system audit log shall contain sufficient information to allow the auditing of all operations related to central site ballot tabulation, results consolidation, and report generation. It shall include a/an • Identification of the program and version being run • Identification of the election file being used • Record of all options entered by the operator • Record of all actions performed by the subsystem • Record of all tabulation and consolidation input	Print a copy of the audit log and verify all items are recorded.	Audit logs printed and all information listed in requirement was printed and verified.
3.23	The system audit log must be created and maintained by the system in the sequence in which operations were performed.	Review audit log after completing successful vote test and ensure each step that used supervisor access is correctly sequenced.	The audit log is generated in sequential order and each transaction within the audit log is time stamped.
3.24	The system audit log must be created and maintained by the system in the sequence in which operations were performed.	Print a copy of the audit log and verify all steps are recorded sequentially.	All steps in the audit log are recorded sequentially.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.25	The system shall provide for safeguards against and evidence of tampering, theft or damage of the system and units.	Review audit logs to verify any act will be recorded and logged with a timestamp.	All actions to the AccuVote-TS are recorded in the audit log with a time stamp. This includes opening and closing the polls, voting, inserting invalid voting cards, loss of power, and supervisor access.
3.26	The media/medium in which vote counts are transferred to the Tally software shall not allow modification of the vote count.	Try to access and modify the vote count on the PCMCIA media or medium (telephone line, etc.) before the vote count is loaded into the GEMS software.	We were unable to alter vote counts on the PCMCIA card, which stores the data. The data is stored in a binary format and it was difficult to read vote records and counts. It was possible to change the data on the PCMCIA card but the AccuVote-TS would not recognize the modified card as valid for the election.
3.27	The system shall ensure that a voter's exact voting record cannot be traced back to the voter.	Try to access the information needed to reconstruct a voter's exact voting record.	Individual vote records are not reported from the AccuVote-TS or tally software. The voting records are not kept in any specific order and the voter is kept anonymous. The system will provide for provisional voting by creating a sequence to list provisional voter records.
3.28	The system shall prevent modification of the voter's vote after the ballot is cast.	Verify vote cannot be altered once the ballot has been cast by using available supervisor functions on the AccuVote-TS.	User cannot alter vote ballots cast. There is no supervisor function to allow for the votes cast to be altered.
3.29	The system shall protect the secrecy of the vote such that the vote may not be observed during the voter's selection of preferences, during the casting of the ballot, and as the voted ballot is transmitted for recording on a storage device.	When the vote is being cast, others should not be allowed to view the voter's selection of preferences.	There are no supervisor functions to allow the view of a voter's selection. The supervisor must close the election to print reports. Curtains protect the voting booth.
3.30	The system shall prohibit voted ballots from being accessed by anyone until after the close of polls.	Verify reports can only be executed after the polls have been closed.	Supervisor functions to print reports are not available until the polls are closed. Reports can only be created after polls have closed.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.31	The system shall provide that each voter's ballot is secret and the voter cannot be identified by image, code or other methods.	Conduct a mock election and cast votes. Close the election and print out a record of each individual vote cast.	Individual vote records are not reports created from the AccuVote-TS. The voting records are listed in no specific order and the voter is kept anonymous. Provisional voting is handled differently. Voter records can be re-constructed to verify if the vote cast is allowed or not allowed. This function is performed on GEMS.
3.32	The system shall provide a summary screen at the end of the ballot showing what the voter has chosen prior to the final vote being cast.	Vote for all issues and/or candidates and before casting the ballot, verify a summary of all votes is presented.	A summary of all votes for each race for the particular user is displayed before we can cast the ballot. Corrections to any race can be made at this point.
3.33	The AccuVote-TS shall not allow unauthorized modification to its operating system.	Try to modify the operating system on the AccuVote-TS by loading a new operating system off the PCMCIA card.	Attempted to load a counterfeit program using the PCMCIA card. Error message was clearly presented to user stating the program cannot be loaded. Error message was generated based on a CRC check of files on the PCMCIA card.
3.34	The DRE shall not allow printing of summary reports before the sequence of events required for closing of the polls are completed.	As a Supervisor, print reports before closing the election.	The DRE will not allow any reports to be created or printed until the election has been closed using a supervisor card.
3.35	There shall be no loss of data during generation of reports including results, images and inaccurate vote counts.	Print out reports after election has been closed and verify no inaccuracies exist.	Printed election reports after the close of the election and verified no results were lost during this function.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.36	The system shall provide printed records regarding the opening and closing of the polls and include the following: • Identification of election, including opening and closing date and times • Identification of each unit • Identification of ballot format • Identification of candidate and/or issue, verifying zero start • Identification of all ballot fields and all special voting options • Summary report of votes cast for each device, or ability to extract same	Close the election and print out a copy of the audit log and review all transactions.	All transactions are captured on the audit logs including specific information about the AccuVote-TS, definition of the election, and all actions occurring on the AccuVote-TS during the election. All items identified in this requirement are present.
3.37	The system shall produce a paper audit trail. To guard against fraud, systems shall not produce individual paper records that voters could remove from the polling place.	Complete and close an election and print out a copy of the audit log from a specific AccuVote-TS.	An audit log is printed out using a specific supervisor function. The audit log produces a report that is a paper trail to guard against fraud.
3.38	The system shall provide printout results containing candidates and/or issues in an alphanumeric format next to the vote totals.	Conduct a mock election and cast multiple votes. Once the voting is closed, print out results of the election using the supervisor functions.	Supervisor must close election and select the option to print votes cast. The printout presents the votes cast in a summary format.
3.39	The system shall allow for extraction of data from memory devices to a central host.	Close the election and transfer results to tally software (GEMS). This is done by connecting the AccuVote-TS to the Tally software through a network connection using a PCMCIA PC adapter card.	Results of ballots cast transferred to GEMS (tally software) with no problems.
3.40	The Tally software shall not allow the double counting of votes from a precinct or AccuVote-TS.	Upload election results from an AccuVote-TS to the tally software. Upload them a second time.	We tried to upload the same results twice to GEMS software. An error message is presented stating the results have already been uploaded.
3.41	The Tally software shall not allow modification of the vote count.	Try to modify the vote tally in the GEMS software using a tool such as MS Excel or MS Access.	A tester was able to view records in the database with a viewer. The tester also altered counts and deleted audit log records using MS Access.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.42	The system shall provide for summary reports of votes cast on each voting device by extracting information from a memory device or a removable data storage device.	Conduct a mock election for two different AccuVote-TS units (or memory devices) and verify a report can be created that list counts for each device.	Supervisor must close election and select the option to print votes cast. This can only be done when election has been closed. Once all AccuVote-TS voting machines have closed all results are uploaded to GEMS where reports are created. Reports can be created to show results for each AccuVote-TS.
3.43	The system shall provide for easily downloading results from balloting into the final tally of votes.	Conduct a mock election and have multiple voters cast ballots. Once the election is closed, the supervisor card must be used to selection the option of transferring votes to GEMS software for tallying and reporting.	Accessed these functions using a supervisor card. The supervisor then uploaded all results of the vote from each AccuVote-TS voting machine.
3.44	The system shall accurately report all votes cast.	Set up a mock election and cast multiple votes. Verify all votes have been included in reports created by GEMS.	All votes cast were included in counts recorded by GEMS software. All reports in GEMS accurately reflect number of votes cast on AccuVote-TS.
3.45	The system shall provide a cumulative, canvass and precinct report of absentee voting, provisional ballot voting and Election Day voting as one total.	Verify election management software has the ability to handle provisional and absentee ballot voting.	Verified that functionality for recording absentee and provisional voting exists in the GEMS software.
3.46	The system shall provide a cumulative, canvass and precinct report of Election Day Voting as one total.	Complete an election. Print the reports from the Host computer.	Printed the reports from the GEMS software. Verified that provisional voting and absentee ballots were included.
3.47	The system shall not lose votes, corrupt media or have performance issues due to the presence of a magnetic field.	A magnet is placed on the LCD unit on the AccuVote-TS smart card reader when voting and PCMCIA slot when recording the votes.	There was no visible degradation on the display. During voting, the magnet did not have any effect on the smart card reader. The PCMCIA card did not get corrupted because of the magnetic field and no votes were lost.

Step 4: Controls Analysis

The Secretary of State has not been required to have a security plan in place for electronic voting systems in the past. As a result of HAVA, the requirement now exists.

Based on the findings of this report and the report developed by InfoSENTRY, the Secretary of State will develop a new security plan or modify the existing security plan to include risk mitigation strategies to minimize or eliminate the likelihood of threat.

Step 5: Threat Likelihood

In Step 5, the assessment team examined the threats identified in Step 2 against each potential vulnerability, and assigned a likelihood rating. The likelihood rating indicates the probability that a potential vulnerability may be exercised, taking into account the nature of the threat, motivation and capability of the threat-source (if human), and existence and effectiveness of current controls.

Each potential vulnerability was assigned a threat likelihood rating of High, Medium, or Low. The following table lists the potential vulnerabilities identified and their likelihood rating.

Potential Vulnerability Identified	Threat Likelihood Rating
Hacking	Medium
System intrusion, break-ins -Physical	Medium
Unauthorized system access- Physical	Medium
Fraudulent act	Low
Information bribery	Low
Spoofing	Low
System intrusion	Medium
Bomb/Terrorism	Low
Information warfare	Low
System attack	Medium
System penetration	Medium
System tampering	Medium
Economic exploitation	Low
Information theft	Medium
Intrusion on personal privacy	Low
Unauthorized system access (access to classified, proprietary, and/or technology-related information)	Medium
Unauthorized system access	Medium
System sabotage	Medium
System bugs	Medium
Malicious code	Medium
Fraud and theft	Low
Input of falsified, corrupted data	Low
Interception	Low

Step 6: Impact Analysis

In Step 6, the assessment team determined the adverse impact(s) that would likely occur if a threat-source were able to successfully exploit a vulnerability or weakness. The team followed the process below to determine the adverse impact resulting from a successful exploitation of a vulnerability:

- Determined the criticality of the electronic voting system and data to accomplishing the SOS' mission.
- Determined the probable adverse impact of a successful exploitation of a vulnerability.
- Determined the adverse impact of a security event in regard to loss or degradation of the system's integrity, availability, and confidentiality.
- Assigned a rating of High, Medium, or Low to each vulnerability to indicate the magnitude of impact resulting from a successful exploitation of the vulnerability.

The following table shows the magnitude of impact rating that was assigned to each potential vulnerability.

Potential Vulnerability Identified	Magnitude of Impact Rating
Code Review	
Third Party Software: The Diebold AccuVote-TS is written with additional third party components. Although the third party software is included in the DRE, Diebold does not maintain the system. There is a potential risk that a security flaw in these third party products could be inadvertently introduced and exploited. In order to exploit a vulnerability it would require the attacker to be able to create, compile and include malicious files on the AccuVote-TS when the firmware is upgraded.	Low
Supervisor Security: The supervisor card has only one PIN that is currently universal throughout the system. If someone was to discover the PIN, and have a valid supervisor smart card then there is a potential risk for affecting the quality of the machine. Though no results can be modified, it can disrupt the election.	Low
Encryption: The Diebold Accuvote-TS does use a DES type of encryption. The key for the encryption is currently hard coded in the system. Using this key it is theoretically possible to be able to decrypt the contents of the removable flash media. The contents of the files that contain votes after decryption are unintelligible.	Low

Continued on the next page

Step 6: Impact Analysis (continued)

Potential Vulnerability Identified	Magnitude of Impact Rating
Platform Review	
Smart Card - with access to a smart card (voter-supervisor) with the proper training and understanding of the smart card, a counterfeit card can be made.	Medium
Smart Card Password - with access to the supervisor card, someone could guess the four digit PIN. The four digit PIN is a factory default from Diebold and cannot be changed. In our test it was guessed in less than two minutes of testing.	High
Smart Card Writer - with access to the small handheld writer, someone could use a voting card more than once while at the voting booth.	High
PCMCIA Card - the cards are not encrypted in any way with DES or PGP Keys to prevent attacks.	Medium
PCMCIA Card - with access to the card and proper training the binary files on the card can be broken and changed.	Medium
Physical Testing	
Diebold's voting system uses MS Access as the database to store the Ballot definition, Audit logs and Tally results. The Database has no password protection. The audit logs and the tally results can be changed.	High
Supervisor smart card has the same PIN for all the elections. Using a supervisor smart card, one can end the elections early, reset the AccuVote-TS, clear the PCMCIA card.	High
PCMCIA card (which stores the ballot definition and results) could be corrupted.	Low

Step 7: Determine Risks

The purpose of Step 7 is to assess the level of risk to the electronic voting system. In this step, the assessment team identified the risk(s), if any, arising out of each test scenario. After identifying the risks, the team assigned a risk rating for each vulnerability by combining the results of the Impact Analysis established in Step 6 with the Likelihood of Threat established in Step 5. The combination of the impact analysis and the threat likelihood versus the security controls in place were applied to a risk-level matrix to determine the resultant risk-level.

Risks Identified

The assessment team identified the following vulnerabilities of the AccuVote-TS voting system. For each vulnerability identified, the table lists the relevant requirement tested, test scenario, and test results which identified the vulnerability.

No.	Test Scenario	Test Result	Risk Identified
Code Review			
1.01	Perform visual review of source files. Function names will be checked for proper case formatting of concatenated words. Names of functions should clearly describe its purpose.	There is a standard for the naming of the code. The naming conventions of the variables and constants across modules are consistent and clear using good coding standards.	None.
1.02	Perform visual review of source files. Modules should contain a consistent format and location for module components. Modules should begin with comments describing the modules contents. Location of methods and variables with associated comments should be consistent throughout.	The modules contain descriptive file names, and descriptions of the tasks performed. The modules appear consistent file to file.	None.
1.03	Perform visual review of source code. Modules should use a clear methodology of construction. Files will be reviewed to see if a coding industry standard is used in the naming of modules, functions, variables and constants.	The construction of the modules is consistent across all files. Components of the modules are easy to identify. In the software specifications it mentions a preference to follow the K&R style and Hungarian notation as well. These formats are closely followed in the source code.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.04	Perform visual review of source code. Function and variable names should be "self documenting" as well as contain properly typed and sized attributes, and return types.	Variables are well named and are clearly used throughout the source code. There is appropriate use of single letter variables in loops.	None.
1.05	Perform visual review of source code for implementation of error handling code. All methods should contain error-handling logic. Systems should remain stable in the event of an error. When an error occurs, sufficient information regarding the state of the system and system parameters should be recorded for future debugging.	The system is written in Visual C++ using Microsoft Foundation Classes. This environment provides C++ statements and MFC classes for error and exception handling. These include the **try**, **catch**, and **throw** statements of Visual C++. Blocks are provided in the software, using these features, to detect and respond to exception and error conditions. If, during system operations, an error or exception condition is detected, either by the system or by some library function, an Exception is thrown. This Exception will then be caught by the first catch block that matches the Exception.	None.
1.06	Perform visual review of source code. Comments will be reviewed for simple descriptive content. Comments should appear at the beginning of each module, function. All module level variables, constants, and structures should be commented as well. Function parameters and return values should describe appropriate values. Comments should also appear in methods to help clarify complex code and logic behind expressions.	Comments do appear at the top of all source modules. Module variables are individually commented or for functional areas. Functions are commented but parameters and return values are, in most instances, not commented. For long and complex methods there are comments helping to clarify long code segments.	None.
1.07	Perform visual review of source code. Comments should have a common format with standard fields for information. Some standard fields should be a description, parameters, return types, a change log.	There is a consistent use of comments through out the code for identifying the functionality of methods. There are descriptions for almost all methods, but additional comments for parameters and return values is not available.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.08	Perform visual review of source code. Modules should have a standard comment identifier at the beginning of each module. Module comments should contain the name and description of the module, a copyright notice, and a change log.	There are comments that begin each module. The comments include the name of the file, the revision history, and a detailed description of the functionality contained in the module.	None.
1.09	Perform visual review of the source code. Modules will be reviewed for their functional content. The variables and functions should be closely related and work directly to perform a clear task.	In reviewing the code modules and the provided software requirements, a close relationship was not found between the source code and the written requirements.	None.
1.10	The source code will be visually reviewed to verify if the code has been properly modularized. Modules should be an appropriate length and encapsulate related functionality.	The source code has been broken into functional areas and then further broken down into individual source modules. Though some modules are long, their size is appropriate.	None.
1.11	The source code will be visually reviewed for the use of simple and clear logical structures. There should be the use of constants (consts) and data structures (structs) to improve code readability and reliability.	The source code does have a lot of use of simple data structure constructs. When a construct is used the internal components are clear and closely related. Variables are passes around by reference for efficiency in memory usage and system speed.	None.
1.12	The source code will be visually reviewed to verify if the code has been properly modularized. Modules should encapsulate related functionality into logical groupings with clear interfaces. Interfaces should be well defined as to their use.	Some of the modules are quite large but they appear to be limited to critical areas of functionality where considerable processing is required. The functionality of modules is well grouped. They are well laid out and easy to follow.	None.
1.13	The source code will be visually reviewed to verify implementation of classes and proper modularization of the source files.	The modularization of the source code appears to be well thought out and appropriate. The groupings of functional elements are clear and well reasoned. Where there are questions as to where to put a component, there are comments describing the quandary and the reasoning behind the decision.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.14	The source code will be visually reviewed. The name and description of the class should be simple and clear. The task performed by the function should be easy to understand, simple to define, and atomic.	The C++ source code has an appropriate use of encapsulation and interfaces. The use of access qualifiers is appropriate to make class interfaces clear, and to understand how to use the modules.	None.
1.15	The source code will be visually reviewed to find any use of third party products. The makers and the versions of any found third party applications will be noted.	There is use of several third party components. Audio playback is from an open source library named Fmod. The version used is not known. Access of the external flash memory is from FlashFx from the Datalight Corporation. Both of these are used as packages and the source code was not available.	None.
1.16	If the source is available for any used third party products, the source will be reviewed for client modifications. Third party source code should only contain the necessary functionality with unused areas removed or disabled. If the source is not available then further study will be required.	Diebold does not maintain the third party packages. Updates come from the owner of the source code. In the case of Fmod, it is an open source package where the source code is freely available to anyone. **Note:** In order to exploit a vulnerability it would require the attacker to be able to create, compile and include malicious files on the AccuVote-TS when the firmware is upgraded.	The Diebold AccuVote-TS and GEMS contain additional third party components. Although the software is included in the AccuVote-TS, Diebold does not maintain these third party components. There is a risk that a security flaw in these third party products could be inadvertently introduced and cause disruption of the election process.
1.17	The data model and database source code will be reviewed for existence of proper keys and normalization.	There is no use of a database on the AccuVote-TS. Data files are stored in internal and external memory as binary flat files.	None.
1.18	The source code will be visually reviewed for user access levels and roles implemented as part of security.	Not applicable to the design of the Diebold AccuVote-TS.	None.
1.19	Source code will be reviewed and tested in order to check for CRC techniques in verifying the correctness of data that is stored in memory. Can the software identify data that has been improperly modified?	The contents of the memory are check summed. The type of checksum is a CRC16 format. The data is verified at the time the ballots are first loaded and after every vote.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.20	The source code will be reviewed to make sure that an algorithm is implemented to make sure voter records are stored in random order. The Cast Vote Records should not have time stamp associated with it.	The votes are stored in a random order into separate vote buckets. The vote records are hashed in a random order to prevent determination of the vote order.	None.
1.21	The source code will be reviewed to verify the system is secure and allows each voter to only vote once by issuing unique access codes.	A voter card controls voter access. The voter card is a smart card issued only from Diebold. Voter cards are activated by using a card reader to properly identify the precinct of the voter. The information on the voter card only allows the DRE to identify and present the proper ballot for the voter . Immediately after voting the card is disabled and ejected from the DRE and the voter is to return the card to the poll workers. The supervisor's access is limited with a Supervisor's card and a PIN must be entered. The PIN is set by Diebold and is the same for all DREs of this type.	a) There is a risk that the unencrypted contents of the smart card may be interpreted by an unauthorized person and used to disrupt the election process. b) The AccuVote-TS supervisor card has an associated PIN provided by Diebold. This PIN is 1111 for all cards issued nationwide. There is a risk that an unauthorized person could learn the PIN number of "1111" on the current version of software and gain access to the supervisor functions on the machine using any Supervisor card.
1.22	The source code will be reviewed to verify there is a means by which votes can be recovered in case of a system disaster.	All results are stored on the removable flash memory. Additionally the results are stored on an internal flash memory that can be removed if needed.	None.
1.23	The strength of encryption will be reviewed. The types of encryption will be reviewed to see if it is sufficient.	Diebold stores ballot definitions and Cast Vote Records on the PCMCIA removable media. The Cast Vote Records are encrypted with a DES encryption package.	None.
1.24	Ballot Definitions and Cast Vote Records should be protected and be verifiable they are correct. Encryption should be powerful enough to block access to stored data.	Diebold stores ballot definitions and Cast Vote Records on the PCMCIA removable media. The contents of the data are encrypted with a DES encryption package.	The ballot definition files do not appear to be encrypted. A DES encryption scheme is used when Cast Vote Records are stored. There is a risk when any data is not encrypted.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.25	Various means of "voter identification" should be secure. The data on a voter authorization token should not be discernable.	Voter smart cards are used to allow access to a AccuVote-TS. The contents of the voter card are not encrypted but access is limited by internal hardware keys that are specific to the system. These keys prevented direct access to the contents of the smart card.	There is a risk that the information on a smart card could be deciphered. No encryption is used in protecting the contents of a smart card. More powerful tools may exist allowing cracking of the Smart Cards' contents.
1.26	Encryption keys should be randomly generated every time and sufficiently long so that it is not easy to guess. The key its self should be kept private and not easily discovered.	The Diebold Accuvote-TS does use a DES type of encryption. The key for the encryption is currently hard coded in the system.	The Diebold AccuVote-TS does use a DES type of encryption. The key for the encryption is currently hard coded in the system. There is a risk that an unauthorized person could decrypt the contents of the removable PCMCIA card using the hardcoded key.
1.27	Transmission protocols will be checked for the use on encryption. Data should never travel over a wire without protection. The contents of the transmission should be verifiable as to their contents and correctness. Any type of tampering should be identifiable if not impossible.	Data is not encrypted when transmitted over a data link.	Data is not encrypted when transmitted over a data link. There is a risk that unencrypted data can be intercepted when transmitted over the data link.
1.28	Check the vote records on the AccuVote-TS, GEMS software, and transfer medium to ensure that the records are encrypted.	Contents of the voting records are encrypted using DES.	None.
1.29	Check the audit logs on the AccuVote-TS to ensure that they are encrypted.	Contents of the audit logs are encrypted using DES.	None.
1.30	Perform code review to ensure that passwords used in all software are encrypted.	There are no passwords that are stored. There is a hard coded system access in the source code.	None.
1.31	Perform code review to ensure that the system does not use hardcoded passwords.	The only password is the supervisor's password and it is hard coded.	Same as 1.21(b) – The AccuVote-TS supervisor card has an associated PIN provided by Diebold. This PIN is 1111 for all cards issued nationwide. There is a risk an unauthorized person with knowledge of this PIN will gain access to a supervisor card and use it to access supervisor functions on the DRE.

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
Platform Review			
2.01	Attempt to convert a valid Voter smart card into a Supervisor smart card that is recognized by the AccuVote-TS.	We were unable to manufacture a counterfeit Voter smart card or to convert a Voter smart card into a Supervisor Card. Using an ACR80 Card Tool purchased on-line we were able to read and write to the EEPROM on both the Voter and Supervisor cards. We changed the default string in the EEPROM from ?@ABCDEF to TacoTest and could then read the value 'TacoTest' back. This was also the case with a valid Voter card with Precinct.001 ballot on it. The EEPROM was able to be read as well as writing the value 'TacoTest' to it. We were able to use the ACOS card player to issue the following commands with successful execution: Start Session, Authenticate, Submit Code, Select File, and Change PIN on both the Voter card and the Supervisor card. These commands completed successfully but the files, records, and code submitted as commands did not return any relevant data even though the commands completed successfully. WE also were able to setup Encryption/Decryption on both cards with the ACR80 Card Tool. We tried to create a counterfeit voter card out of a blank ACS smart card on the AccuVote-TS. The response was: Please remove the Voter Card and try again or press Cancel to abort. Finally we tried to create a Voter Card out of a third party card and the response was: Card upside down or not inserted correctly. Please remove the Voter Card and try again or press Cancel to abort.	We were unable to counterfeit a Voter smart card or convert a Voter smart card into a Supervisor Card with the equipment we had available. This does not prove a working smart card cannot be counterfeited but does indicate it is not an easy task to accomplish. There is a risk that an unauthorized person might be able to create and use a counterfeit smart card to access supervisory functions or cast extra ballots.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
2.02	Try to modify the Ballot Definition file on the PCMCIA card before loading it on the AccuVote-TS. Try to modify the card using a simple laptop and then insert it in the AccuVote-TS.	File would not load from the PCMCIA card. The system warned of a bad file and would not load the files from the card. The AccuVote-TS recognized that the files were changed on something other than the AccuVote-TS or voting software.	The AccuVote-TS uses a standard PCMCIA card which can be inserted in a Windows PC. When files were modified, the files would not load from the PCMCIA card. The system warned of a bad file and would not load the files from the card. There is a risk that an election-ready PCMCIA card might be corrupted using a laptop PC resulting in disruption of the voting process.
2.03	Install a program on a PCMCIA card, insert it in the AccuVote-TS, and install and/or execute the unauthorized program.	The system would not load an executable file by itself, and attempts to use the Win CE to find the file on the PCMCIA card were unsuccessful.	None.
2.04	Inspect the AccuVote-TS for network accessible ports.	The AccuVote-TS connects to the network through a PCMCIA network card with Windows CE TCP/IP protocols. This is the normal port for loading ballot definitions and uploading cast ballot records.	A network port is provided for loading the ballot definitions and uploading cast vote records. This should be done on a point to point network. There is a risk that if the AccuVote-TS is connected to an unsecured internet or intranet, the AccuVote-TS could be compromised.
2.05	Try to access, modify, or disrupt the functioning of the AccuVote-TS software while connected to a network.	A laptop computer was connected to the network with an AccuVote-TS and GEMS server. Several attempts were made to gain control of or modify information on the AccuVote-TS from the laptop. None of these attempts were successful at accessing the information within the AccuVote-TS.	None.
2.06	Try to bring the system down, lock up the operating system, change or erase log files, or any other form of Denial of Service (DoS), Distributed Denial of Service (DDos), or other result which benefits the attacker.	The system has a lock and key in place to covered ports and system reset. Could not tamper with system while lock cover in place and keyboard attached. If the cover is open, the operating system and/or the application, BallotStation.exe, can be locked up by pressing the function key F4 which brings up the Open File dialog box. By navigating to \FFX\Bin and invoking BallotStation.exe the system locks up or freezes.	Ports on the AccuVote-TS are covered by a locking panel. There is a risk that if the cover is unlocked during an election, the exposed ports could be used to disrupt the AccuVote-TS.

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
2.07	Try to gain supervisor rights or system rights by any means necessary.	Tests were preformed to change a voter smart card to supervisor card. We were able to read and write to the Diebold card but we could not change the voter card to a valid supervisor card with a smart card reader and writer.	We were unable to counterfeit a Voter smart card or convert a Voter smart card into a Supervisor Card with the equipment we had available. This does not prove a working smart card cannot be counterfeited but does indicate it is not an easy task to accomplish. There is a risk that an unauthorized person might be able to create and use a counterfeit smart card to access supervisory functions or cast extra ballots.
2.08	Try to cause a kernel panic, system failure, or indefinite wait state, or other operating system lock-up within the operating system or sub-system. With the access panel open and a keyboard or keypad plugged in, multiple or simultaneous keystrokes hit or key combinations pressed simultaneously was the main method of attack.	No attempts could be made while the cover was locked. When the cover was open, ports were available but we were unable to produce any kernel panics, wait states, or other operating system lock-ups, freezes, or general protection faults or invalid page faults in the AccuVote-TS.	None.
2.09	Observe that functions are password protected, the minimum length of passwords, and that they can be changed.	The password or PIN used for the supervisor smart card is the same for all cards by Diebold. It is a four-digit number and was guessed on the third attempt, and we gained access to the supervisor functions on the AccuVote-TS. The four-digit PIN is a factory default from Diebold and cannot be changed.	Same as 1.21(b) – The AccuVote-TS supervisor card has an associated PIN provided by Diebold. This PIN is 1111 for all cards issued nationwide. There is a risk an unauthorized person with knowledge of this PIN will gain access to a supervisor card and use it to access supervisor functions on the DRE.
2.10	Try to create an attack on flash memory using files loaded on the PCMCIA card.	File would not load from the PCMCIA card. The system warned of a bad file and would not load the files from the card. The AccuVote-TS recognized that the files were changed on something other than the AccuVote-TS or voting software.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
2.11	Change the contents on a removable media card and use the card. Determine if the system reports the card has been modified.	When the clear text parts of a binary file were changed, the system recognized it as a bad file and would not load it onto the AccuVote-TS.	None.
2.12	Try to modify protective counter.	There was no way to access the protective counter through ports, PCMCIA card or Supervisor smart card via telnet, FTP, voter card changes, or additions to the PCMCIA card to change the protective counter.	None.
2.13	Examine the hardware and communication architecture to determine if TCP hijacking attacks are possible.	The AccuVote-TS is not on a network and uses a direct connection to the management software within a few feet.	A network port is provided for loading the ballot definitions and downloading cast vote records. This should be done on a point to point network. There is a risk of a TCP hijacking attack if the AccuVote-TS is connected to an intranet or internet.
2.14	Try to gain access via an open TCP/UDP or serial or USB or other port.	An Nmap scan revealed: the following ports/services were filtered: 21/tcp-ftp, 389/tcp-ldap, 1720/tcp-H.323/Q.931(where H.323 is the teleconferencing protocol for voice/data/video IP telephony). Filtered ports are usually covered by a firewall, filter or other device. The following ports are also open (where an open port is defined as “will accept connections on that port”): 21/tcp-ftp, 25/tcp-smtp, 110/tcp-pop3, 389/tcp-ldap, 1002/tcp-unknown, 1720/tcp-H.323/Q.931 (Q.931 is a ISDN connection control protocol).	Same as 2.06 - Ports on the AccuVote-TS are covered by a locking panel. There is a risk that if the cover is unlocked during an election, the exposed ports could be used to disrupt the AccuVote-TS.
2.15	Try to introduce any type of malicious software (malware) into the system.	Putting a program on a PCMCIA card did not work since the system would not load it. Attempts to load a program through an open port were unsuccessful.	None.
2.16	Inspect the hardware design documents and physical hardware.	The system was sealed shut with no access to the flash memory. When the PCMCIA card slot is locked, there is no way to access it without the key.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
2.17	Inspect the physical hardware for location of seals and locks and for safeguards against and evidence of tampering.	The unit provides for an external lock and/or seal which would prevent undetected tampering, provided duplicate seals were not available.	None.
2.18	Voted on unit, then removed power. The unit was left on overnight to drain the battery. The unit was started back up and checked for correct data.	When power was pulled or drained the memory was kept on the flash. No voting data was lost or corrupted.	None.
Physical Testing			
3.01	Check PCMCIA card to determine whether it can be removed easily and can be locked.	The PCMCIA card is housed in a lockable compartment and it cannot be removed when locked.	There is a risk that the PCMCIA card can be removed if the compartment is not locked.
3.02	Conduct logic and accuracy tests and verify system audit information is present.	Accuracy and logic tests were conducted before the election. System audit information is displayed on the resulting print out.	None.
3.03	Conduct logic and accuracy test and verify results are recorded in the on-board memory by printing the audit log.	Accuracy and logic tests were conducted before the election to verify system information was correct. Logic and accuracy test result were printed in the audit log.	None.
3.04	Conduct logic and accuracy testing before election is started. Print a zero tape before an election and a result tape after an election.	Accuracy and logic tests were conducted before the election to verify counters are working properly and the programming for each voting device is correct. A zero tape printout was created and verified that no votes were cast before the start of the election. After voting was closed, a result tape was printed.	None.
3.05	Create an instance where a known error will occur on the AccuVote-TS. For instance, enter a voter card after it has been de-activated.	AccuVote-TS displays a concise error message. This is standard throughout all error handling functions on the AccuVote-TS.	None.
3.06	Conduct a logic and accuracy test.	Accuracy and logic tests were conducted before the election to verify counters are working properly and the programming for each voting device is correct.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.07	Try to modify the Ballot Definition in the GEMS software using a database viewer/program.	We were capable of viewing the ballot definition file through Microsoft Access. Changes could be made to the database and all records can be viewed. The audit log is also stored in the database and could be viewed and edited.	GEMS uses the MS Access database to store ballot definition data and election results. There is a risk that an unauthorized person with access to the GEMS server can access the database and change ballot definition files and election results.
3.08	Create an election ballot definition file and transfer the file to the AccuVote-TS. Open election and look at ballot.	The ballot is presented in a clear and unambiguous manner.	None.
3.09	Insert a counterfeit smart card into the AccuVote-TS and try to use it to vote.	Unable to produce a working counterfeit smart card.	None.
3.10	Insert an authorized smart card into the AccuVote-TS and try to use it to vote multiple times.	Once a vote has been cast, the smart card used is deactivated. When trying to insert the deactivated smart card to vote again, the card is ejected from the reader.	None.
3.11	Create a counterfeit Voter Access smart card then attempt to use it so it is recognized and authenticated by the AccuVote-TS.	Unable to produce a working counterfeit smart card.	None.
3.12	Insert a supervisor card in the AccuVote-TS and try to view or change vote results.	The supervisor menu does not allow a user to change or view vote results. Results can only be viewed and/or printed after election has been closed.	None.
3.13	Insert a Supervisor Card in the AccuVote-TS and try to terminate the election early.	With the use of a supervisor card and the correct PIN number, we were able to close the election early. Inserted the supervisor card, entered the four-digit pin, and the AccuVote-TS prompted, “Do you want to close the polls? Yes/No”.	The AccuVote-TS supervisor card has an associated PIN provided by Diebold. This PIN is 1111 for all cards issued nationwide. There is a risk an unauthorized person with knowledge of this PIN will gain access to a supervisor card and use it to close the polls early.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.14	Insert a Supervisor card in the AccuVote-TS and try to reset the AccuVote-TS.	The AccuVote-TS cannot be reset during voting. Once voting is closed, the AccuVote-TS can be reset with a supervisor card and the correct PIN number. Resetting clears the memory on the AccuVote-TS and can clear the PCMCIA card as well.	None.
3.15	Insert an authorized supervisor card in the AccuVote-TS and try to access supervisor functions using an incorrect PIN.	User is denied access when using an incorrect PIN. An error message is clearly displayed to the user. The supervisor PIN number is the same for all supervisor cards distributed by Diebold and was guessed in three tries during our testing.	None.
3.16	Start voting on the AccuVote-TS, and then disconnect batteries/power for 30 minutes to simulate a power outage, Resume power and start up the AccuVote-TS, and check the voter information.	Removed power cord and AccuVote-TS voting machine has a battery backup that powered the machine. The battery is sealed within the machine and could not be removed.	None.
3.17	Start voting on the AccuVote-TS, and then disconnect power for thirty minutes to simulate a power outage, and then resume power. Cast votes before, during, and after the disruption.	Removed power cord and AccuVote-TS voting machine has a battery backup that powered the machine. The battery is sealed within the machine and could not be removed.	None.
3.18	Try to modify the protective counter on the AccuVote-TS.	Supervisor functions will not allow the altering of counts on the AccuVote-TS voting machine. Counter is stored within the CPU on the AccuVote-TS. The number on the counter is printed out before the election and after the election as well.	None.
3.19	Modify the AccuVote-TS so that only core flash memory is available and see if the system will allow voting.	User is prompted to turn off machine or insert memory card. The system will not allow only one memory source.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.20	Try to convert a Voter Access card to a Supervisor card then access and perform supervisor functions in the AccuVote-TS.	Unable to convert a Voter Access card to a Supervisor card.	None.
3.21	Review audit log after completing successful vote test and ensure each step that used supervisor access is correctly logged.	Each time a supervisor card is used, the action is logged within the audit logs specific to the AccuVote-TS.	None.
3.22	Print a copy of the audit log and verify all items are recorded.	Audit logs printed and all information listed in requirement was printed and verified.	None.
3.23	Review audit log after completing successful vote test and ensure each step that used supervisor access is correctly sequenced.	The audit log is generated in sequential order and each transaction within the audit log is time stamped.	None.
3.24	Print a copy of the audit log and verify all steps are recorded sequentially.	All steps in the audit log are recorded sequentially.	None.
3.25	Review audit logs to verify any act will be recorded and logged with a timestamp.	All actions to the AccuVote-TS are recorded in the audit log with a time stamp. This includes opening and closing the polls, voting, inserting invalid voting cards, loss of power, and supervisor access.	None.
3.26	Try to access and modify the vote count on the PCMCIA media or medium (telephone line, etc.) before the vote count is loaded into the GEMS software.	We were unable to alter vote counts on the PCMCIA card, which stores the data. The data is stored in a binary format and it was difficult to read vote records and counts. It was possible to change the data on the PCMCIA card but the AccuVote-TS would not recognize the modified card as valid for the election.	The AccuVote-TS uses a standard PCMCIA card which can be inserted in a Windows PC. When files were modified, the files would not load from the PCMCIA card. The system warned of a bad file and would not load the files from the card. There is a risk that an election-ready PCMCIA card might be corrupted using a laptop PC resulting in disruption of the voting process.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.27	Try to access the information needed to reconstruct a voter's exact voting record.	Individual vote records are not reported from the AccuVote-TS or tally software. The voting records are not kept in any specific order and the voter is kept anonymous. The system will provide for provisional voting by creating a sequence to list provisional voter records.	None.
3.28	Verify vote cannot be altered once the ballot has been cast by using available supervisor functions on the AccuVote-TS.	User cannot alter vote ballots cast. There is no supervisor function to allow for the votes cast to be altered.	None.
3.29	When the vote is being cast, others should not be allowed to view the voter's selection of preferences.	There are no supervisor functions to allow the view of a voter's selection. The supervisor must close the election to print reports. Curtains protect the voting booth.	None.
3.30	Verify reports can only be executed after the polls have been closed.	Supervisor functions to print reports are not available until the polls are closed. Reports can only be created after polls have closed.	None.
3.31	Conduct a mock election and cast votes. Close the election and print out a record of each individual vote cast.	Individual vote records are not reports created from the AccuVote-TS. The voting records are listed in no specific order and the voter is kept anonymous. Provisional voting is handled differently. Voter records can be re-constructed to verify if the vote cast is allowed or not allowed. This function is performed on GEMS.	None.
3.32	Vote for all issues and/or candidates and before casting the ballot, verify a summary of all votes is presented.	A summary of all votes for each race for the particular user is displayed before we can cast the ballot. Corrections to any race can be made at this point.	None.
3.33	Try to modify the operating system on the AccuVote-TS by loading a new operating system off the PCMCIA card.	Attempted to load a counterfeit program using the PCMCIA card. Error message was clearly presented to user stating the program cannot be loaded. Error message was generated based on a CRC check of files on the PCMCIA card.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.34	As a Supervisor, print reports before closing the election.	The AccuVote-TS will not allow any reports to be created or printed until the election has been closed using a supervisor card.	None.
3.35	Print out reports after election has been closed and verify no inaccuracies exist.	Printed election reports after the close of the election and verified no results were lost during this function.	None.
3.36	Close the election and print out a copy of the audit log and review all transactions.	All transactions are captured on the audit logs including specific information about the AccuVote-TS, definition of the election, and all actions occurring on the AccuVote-TS during the election. All items identified in this requirement are present.	None.
3.37	Complete and close an election and print out a copy of the audit log from a specific AccuVote-TS.	An audit log is printed out using a specific supervisor function. The audit log produces a report that is a paper trail to guard against fraud.	None.
3.38	Conduct a mock election and cast multiple votes. Once the voting is closed, print out results of the election using the supervisor functions.	Supervisor must close election and select the option to print votes cast. The printout presents the votes cast in a summary format.	None.
3.39	Close the election and transfer results to tally software (GEMS). This is done by connecting the DRE to the Tally software through a network connection using a PCMCIA PC adapter card.	Results of ballots cast transferred to GEMS (tally software) with no problems.	None.
3.40	Upload election results from a DRE to the tally software. Upload them a second time.	We tried to upload the same results twice to GEMS software. An error message is presented stating the results have already been uploaded.	None.
3.41	Try to modify the vote tally in the GEMS software using a tool such as MS Excel or MS Access.	A tester was able to view records in the database with a viewer. The tester also altered counts and deleted audit log records using MS Access.	Same as 3.07 - GEMS uses the MS Access database to store ballot definition data and election results. There is a risk that an unauthorized person with access to the GEMS server can access the database and change ballot definition files and election results.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.42	Conduct a mock election for two different AccuVote-TS's (or memory devices) and verify a report can be created that list counts for each device.	Supervisor must close election and select the option to print votes cast. This can only be done when election has been closed. Once all AccuVote-TS voting machines have closed all results are uploaded to GEMS where reports are created. Reports can be created to show results for each AccuVote-TS.	None.
3.43	Conduct a mock election and have multiple voters cast ballots. Once the election is closed, the supervisor card must be used to selection the option of transferring votes to GEMS software for tallying and reporting.	Accessed these functions using a supervisor card. The supervisor then uploaded all results of the vote from each AccuVote-TS.	None.
3.44	Set up a mock election and cast multiple votes. Verify all votes have been included in reports created by GEMS.	All votes cast were included in counts recorded by GEMS software. All reports in GEMS accurately reflect number of votes cast on AccuVote-TS.	None.
3.45	Verify election management software has the ability to handle provisional and absentee ballot voting.	Verified that functionality for recording absentee and provisional voting exists in the GEMS software.	None.
3.46	Complete an election. Print the reports from the Host computer.	Printed the reports from the GEMS software. Verified that provisional voting and absentee ballots were included.	None.
3.47	A magnet is placed on the LCD unit on the AccuVote-TS smart card reader when voting and PCMCIA slot when recording the votes.	There was no visible degradation on the display. During voting, the magnet did not have any effect on the smart card reader. The PCMCIA card did not get corrupted because of the magnetic field and no votes were lost.	None.

Risk Levels of Identified Risks

Each Threat-Source/Vulnerability was assigned a rating of High, Medium, or Low to represent the degree or level of risk to which the electronic voting system might be exposed if a given vulnerability were exercised. Following is a description of the High, Medium, and Low ratings.

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, it must determined whether corrective actions are still required or whether the risk can be accepted.

The following table shows the rating assigned to each identified risk.

No.	Risk Identified	Risk Likelihood	Impact Rating	Risk Level
Code Review				
1.16	The Diebold AccuVote-TS and GEMS contain additional third party components. Although the software is included in the AccuVote-TS, Diebold does not maintain these third party components. There is a risk that a security flaw in these third party products could be inadvertently introduced and cause disruption of the election process.	Low	High	Low
1.21(a)	There is a risk that the unencrypted contents of the smart card may be interpreted by an unauthorized person and used to disrupt the election process.	Low	Low	Low
1.21(b) 1.31	There is a risk that an unauthorized person could learn the PIN number of "1111" on the current version of software and gain access to the supervisor functions on the machine using any Supervisor card.	High	High	High
1.24	The ballot definition files do not appear to be encrypted. A DES encryption scheme is used when Cast Vote Records are stored. There is a risk when any data is not encrypted.	Low	Low	Low
1.25	There is a risk that the information on a smart card could be deciphered. No encryption is used in protecting the contents of a smart card. More powerful tools may exist allowing cracking of the Smart Cards' contents.	Medium	Medium	Medium
1.26	The Diebold AccuVote-TS does use a DES type of encryption. The key for the encryption is currently hard coded in the system. There is a risk that an unauthorized person could decrypt the contents of the removable PCMCIA card using the hardcoded key.	Medium	Low	Low

Continued on the next page

Risk Levels of Identified Risks (continued)

No.	Risk Identified	Risk Likelihood	Impact Rating	Risk Level
1.27	Data is not encrypted when transmitted over a data link. There is a risk that unencrypted data can be intercepted when transmitted over the data link.	Low	Medium	Low
Platform Review				
2.01	There is a risk that an unauthorized person might be able to create and use a counterfeit smart card to access supervisory functions or cast extra ballots.	Low	Medium	Medium
2.02	The AccuVote-TS uses a standard PCMCIA card which can be inserted in a Windows PC. When files were modified, the files would not load from the PCMCIA card. The system warned of a bad file and would not load the files from the card. There is a risk that an election-ready PCMCIA card might be corrupted using a laptop PC resulting in disruption of the voting process.	Low	Low	Low
2.04	A network port is provided for loading the ballot definitions and uploading cast vote records. This should be done on a point to point network. There is a risk that if the AccuVote-TS is connected to an unsecured internet or intranet, the AccuVote-TS could be compromised.	High	High	High
2.06 2.14	Ports on the AccuVote-TS are covered by a locking panel. There is a risk that if the cover is unlocked during an election, the exposed ports could be used to disrupt the AccuVote-TS.	Low	High	Low
2.07	We were unable to counterfeit a Voter smart card or convert a Voter smart card into a Supervisor smart card with the equipment we had available. This does not prove a working smart card cannot be counterfeited but does indicate it is not an easy task to accomplish. There is a risk that an unauthorized person might be able to create and use a counterfeit smart card to access supervisory functions or cast extra ballots.	Low	Medium	Medium
2.09	Same as 1.21(b) under the Code Review section above.			
2.13	A network port is provided for loading the ballot definitions and downloading cast vote records. This should be done on a point to point network. There is a risk of a TCP hijacking attack if the AccuVote-TS is connected to an intranet or internet.	High	High	High

Continued on the next page

Risk Levels of Identified Risks (continued)

No.	Risk Identified	Risk Likelihood	Impact Rating	Risk Level
Physical Testing				
3.01	There is a risk that the PCMCIA card can be removed if the compartment is not locked.	Low	High	Low
3.07 3.41	GEMS uses the MS Access database to store ballot definition data and election results. There is a risk that an unauthorized person with access to the GEMS server can access the database and change ballot definition files and election results.	High	High	High
3.13	The AccuVote-TS supervisor card has an associated PIN provided by Diebold. This PIN is 1111 for all cards issued nationwide. There is a risk an unauthorized person with knowledge of this PIN will gain access to a supervisor card and use it to close the polls early.	High	High	High
3.26	The AccuVote-TS uses a standard PCMCIA card which can be inserted in a Windows PC. When files were modified, the files would not load from the PCMCIA card. The system warned of a bad file and would not load the files from the card. There is a risk that an election-ready PCMCIA card might be corrupted using a laptop PC resulting in disruption of the voting process.	Low	Medium	Low

Step 8: Risk Mitigation Strategies

In Step 8, the assessment team recommended solutions that are intended to mitigate or eliminate the risks identified in Step 7. The goal of the recommended risk mitigation strategies is to reduce the level of risk to the electronic voting system and its data to an acceptable level.

Recommended Risk Mitigation Strategies

The assessment team recommends the following mitigation strategies for the risks identified during this assessment.

Code Review

No.	Risk Identified	Recommended Mitigation Strategy
High Risk		
1.21(b) 1.31	The AccuVote-TS supervisor card has an associated PIN provided by Diebold. This PIN is 1111 for all cards issued nationwide. There is a risk an unauthorized person with knowledge of this PIN will gain access to a supervisor card and use it to access supervisor functions on the DRE.	We recommend the Secretary of State require Diebold to provide software access for changing of the supervisor PIN. It is recommended that the PIN be at least six characters in length.
Medium Risk		
1.25	There is a risk that the information on a smart card could be deciphered. No encryption is used in protecting the contents of a smart card. More powerful tools may exist allowing cracking of the Smart Cards' contents.	We recommend the Secretary of State require that Diebold provide encryption on the smart card.

Continued on the next page

Recommended Risk Mitigation Strategies (continued)

Code Review (continued)

No.	Risk Identified	Recommended Mitigation Strategy
Low Risk		
1.16	The Diebold AccuVote-TS and GEMS contain additional third party components. Although the software is included in the AccuVote-TS, Diebold does not maintain these third party components. There is a risk that a security flaw in these third party products could be inadvertently introduced and cause disruption of the election process.	We recommend the Secretary of State require that Diebold maintain configuration management of third party software in the development environment. We recommend the Secretary of State require that an independent security assessment be conducted on each release of the Accuvote-TS.
1.21(a)	There is a risk that the unencrypted contents of the smart card may be interpreted by an unauthorized person and used to disrupt the election process.	We recommend the Secretary of State require that Diebold provide encryption on the smart card.
1.24	The ballot definition files do not appear to be encrypted. A DES encryption scheme is used when Cast Vote Records are stored. There is a risk when any data is not encrypted.	We recommend the Secretary of State require that Diebold provide encryption for ballot definition files.
1.26	The Diebold AccuVote-TS does use a DES type of encryption. The key for the encryption is currently hard coded in the system. There is a risk that an unauthorized person could decrypt the contents of the removable PCMCIA card using the hardcoded key.	We recommend the Secretary of State require that Diebold does not hard code any encryption keys in the software.
1.27	Data is not encrypted when transmitted over a data link. There is a risk that unencrypted data can be intercepted when transmitted over the data link.	We recommend the Secretary of State require that Diebold provide VPN functionality from the AccuVote-TS to the voting software.

Recommended Risk Mitigation Strategies (continued)

Platform Review

No.	Risk Identified	Recommended Mitigation Strategy
High Risk		
2.04	A network port is provided for loading the ballot definitions and uploading cast vote records. This should be done on a point to point network. There is a risk that if the AccuVote-TS is connected to an unsecured internet or intranet, the AccuVote-TS could be compromised.	We recommend the Secretary of State require that administrative policies and procedures be put in place to ensure the AccuVote-TS is not connected to the internet or to an intranet.
2.09	Same as 1.21(b) under the Code Review section above.	Same as 1.21(b) under the Code Review section above.
2.13	A network port is provided for loading the ballot definitions and uploading cast vote records. This should be done on a point to point network. There is a risk of a TCP hijacking attack if the AccuVote-TS is connected to an intranet or internet.	We recommend the Secretary of State require that administrative policies and procedures be put in place to ensure the AccuVote-TS is not connected to the internet or to an intranet.
Medium Risk		
2.01 2.07	We were unable to counterfeit a Voter smart card or convert a Voter smart card into a Supervisor Card with the equipment we had available. This does not prove a working smart card cannot be counterfeited but does indicate it is not an easy task to accomplish. There is a risk that an unauthorized person might be able to create and use a counterfeit smart card to access supervisory functions or cast extra ballots.	We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk. We also recommend the Secretary of State require Diebold to provide software access for changing of the supervisor PIN. It is recommended that the PIN be at least six characters in length.

Continued on the next page

Recommended Risk Mitigation Strategies (continued)

Platform Review (continued)

No.	Risk Identified	Recommended Mitigation Strategy
Low Risk		
2.02	The AccuVote-TS uses a standard PCMCIA card which can be inserted in a Windows PC. When files were modified, the files would not load from the PCMCIA card. The system warned of a bad file and would not load the files from the card. There is a risk that an election-ready PCMCIA card might be corrupted using a laptop PC resulting in disruption of the voting process.	We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk.
2.06 2.14	Ports on the AccuVote-TS are covered by a locking panel. There is a risk that if the cover is unlocked during an election, the exposed ports could be used to disrupt the AccuVote-TS.	We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk.

Physical Testing

No.	Risk Identified	Recommended Mitigation Strategy
High Risk		
3.07 3.41	GEMS uses the MS Access database to store ballot definition data and election results. There is a risk that an unauthorized person with access to the GEMS server can access the database and change ballot definition files and election results.	We recommend the Secretary of State require administrative policies and procedures that limit log-on access to the GEMS server. We also recommend the Secretary of State require administrative policies and procedures be put in place which limit the computer programs and tools available on the GEMS server. These policies should limit use of the GEMS server to executing GEMS.

Continued on the next page

Recommended Risk Mitigation Strategies (continued)

Physical Testing (continued)

No.	Risk Identified	Recommended Mitigation Strategy
3.13	The AccuVote-TS supervisor card has an associated PIN provided by Diebold. This PIN is 1111 for all cards issued nationwide. There is a risk an unauthorized person with knowledge of this PIN will gain access to a supervisor card and use it to close the polls early.	We recommend the Secretary of State require Diebold to provide software access for changing of the supervisor PIN. It is recommended that the PIN be at least six characters in length.
Medium Risk		
N/A		
Low Risk		
3.01	There is a risk that the PCMCIA card can be removed if the compartment is not locked.	We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk.
3.26	Same as 2.02 under the Platform Review section above.	Same as 2.02 under the Platform Review section above.

Step 9: Document Results

In Step 9, the assessment team combined the results of Steps 1 through 8 to develop this report detailing the technical security assessment and its findings.

Conclusion

Compuware has conducted a study of the Diebold AccuVote-TS voting system to identify specific security vulnerabilities that might be exploited during an election and to recommend actions to mitigate these vulnerabilities. The scope of this study has been limited to reviewing the technical implementation of the AccuVote-TS and reviewing each data stream into and from the AccuVote-TS. It has not included a review of the policies, procedures, or work practices of either Diebold or the Ohio Secretary of State.

During the course of our study, Compuware has identified several significant security issues, which left unmitigated would provide an opportunity for an attacker to disrupt the election process or throw the election results into question. These are documented above. Following careful consideration of each of these security issues, we have developed mitigation recommendations for the Secretary of State to implement which we believe will limit the likelihood of a successful attack on the election process. Provided each of these mitigation recommendations can be enacted, Compuware has concluded the Diebold AccuVote-TS can be securely deployed by the Secretary of State.

Although all risks documented above must be dealt with appropriately, the most significant risk areas, which will require the most effort to mitigate, include:

Risk Identified	Recommended Mitigation Strategy
Diebold sets the PIN on all supervisor cards to "1111". Further, any supervisor card will function on any DRE in any election. There is a risk that an unauthorized person with knowledge of the PIN and access to a Supervisor card might gain access to the supervisor functions on any DRE.	We recommend the Secretary of State require Diebold to provide software access for changing of the supervisor PIN. It is recommended that the PIN be at least six digits in length.
Diebold uses a standard PCMCIA card for storing the ballot definitions and vote results. These cards can be easily placed in a laptop and altered. Due to protections in place, the altered card is unreadable by the DRE or GEMS election management software. There is a risk that an election-ready PCMCIA card might be corrupted using a laptop PC.	We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk.
A network port is provided on the AccuVote-TS to download ballot definitions and upload results. There is a risk that if the AccuVote-TS is connected to an unsecured internet or intranet, the AccuVote-TS could be compromised.	We recommend the Secretary of State require that administrative policies and procedures be put into place to ensure the AccuVote-TS must never be connected to the internet or to an intranet.

Continued on the next page

Conclusion (continued)

Risk Identified	Recommended Mitigation Strategy
GEMS uses Microsoft Access to store data used to create ballot definitions and tally results. Microsoft Access databases can be viewed and modified using an external product such as Excel or MS Access. There is a risk that a user with access to the GEMS server can access the database and change ballot definition and voting result records.	We recommend the Secretary of State require that the GEMS server use proper Windows security to prevent unauthorized access, and not contain any additional software that would allow access to the GEMS database.
The AccuVote-TS will allow polls to be closed at any time by a user with a supervisor card and the correct PIN. No warning is given if the polls are being closed early. There is a risk that an unauthorized person can close the polls early if the person gains access to a supervisor card and the correct PIN.	We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk.

Election policies and procedures have long been used to ensure fair and accurate election results. The deployment of DRE technology will not lessen the need for well thought out and consistently enforced policies and procedures.

This page intentionally left blank.

PART THREE: ES&S

Overview

This section details the assessment for the ES&S iVotronic Touch Screen Voting System. The iVotronic is portable, wireless, and multilingual. Its Audio Ballot supports voters who are visually impaired, and its portability enables curbside voting and wheelchair access voting.

The iVotronic is supported by the Unity Election System (UES) software for election management. Unity enables a client to: create and maintain a central database of jurisdiction and election information; format ballot layouts and program election equipment for use in conducting voting within a jurisdiction; and collect, accumulate and report the voting results files directly from the tabulation equipment.

The iVotronic prevents the voter from overvoting, notifies the voter of undervoting, and allows the voter to review and modify their ballot choices before casting their vote.

Compuware tested the following hardware and software in this technical security assessment:

Hardware	Software
IVotronic version 7.4.5.0	Unity Election System (UES) software version 2.2

Step 1: Characterization of the iVotronic Voting System

In Step 1, the iVotronic was examined for the following:

- IVotronic system interfaces – input/output connections between the iVotronic and external entities, and the related voting processes
- Work flow / process model – flow of data through the iVotronic system interfaces, and the related voting processes
- iVotronic environment
    - Hardware configuration
    - Software configuration
    - Network configuration

iVotronic System Interfaces

The following diagram provides a graphical overview of the connections to the iVotronic. The diagram shows the input/output connections between the iVotronic and external entities such as the BOE's and voters.

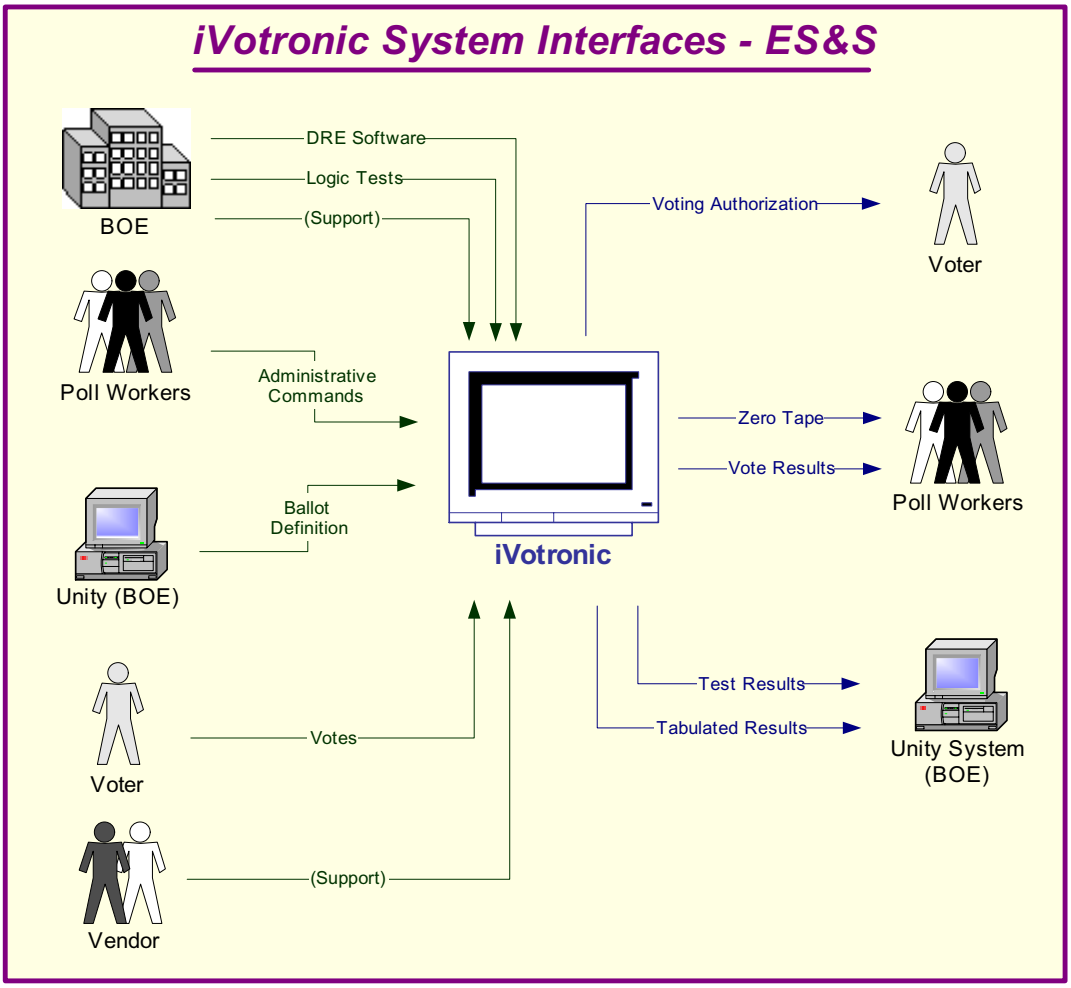

Figure 7 *- iVotronic System Interfaces - ES&S*

Continued on the next page

iVotronic System Interfaces (continued)

Following is an explanation of the tasks related to the iVotronic system interfaces.

Inputs	Outputs
Board of Elections	
• Unity Election System software is installed on a computer at the Board of Elections (BOE). • The BOE uses the Unity software to load information onto the Personal Electronic Ballot (PEB) using the Supervisor iVotronic system.	
• Workers at the BOE enter data into the Supervisor iVotronic and download the results into the PEB to perform the logic and accuracy testing (LAT). • If there is a problem, the BOE troubleshoots the problem and determines if county workers can solve the problem or if the vendor needs to be called.	Workers at the board verify the results that were entered in the LAT.
Vendor	
If there is a problem with the LAT, the vendor may be called in to repair the unit. If the unit is repaired, it must successfully go through the LAT before it may be used in an election.	
Poll Workers	
• Poll workers set up the booth. • Poll workers open the iVotronic for voting using the PEB. • Poll workers authorize the voter to vote by using the PEB and selecting the correct ballot for the voter.	Poll workers print a zero tape from the PEB to ensure there are no pre-existing votes recorded on it. The PEB will print reports for all iVotronics opened with the PEB.
Voter	
Voter votes the ballot. The iVotronic prevents the voter from overvoting, notifies of undervoting, and presents the ballot choices for review as appropriate.	
Poll Workers	
	• Poll workers use the PEB to close all of the iVotronics. • At the last unit, poll workers print a result tape from the information stored on the PEB. • Poll workers post one result tape at the precinct. • Poll workers send the PEB and a copy of the result tape to the BOE.
Board of Elections	
	• The BOE places the PEB in a Supervisor's PEB, and the Unity software counts the votes. • The BOE prints and releases the results.

Work Flow / Process Model

The following diagram provides a graphical overview of the work flow associated with the iVotronic system interfaces, and represents the next level down from the Context Diagram. This diagram displays the flow of data through the iVotronic system interfaces.

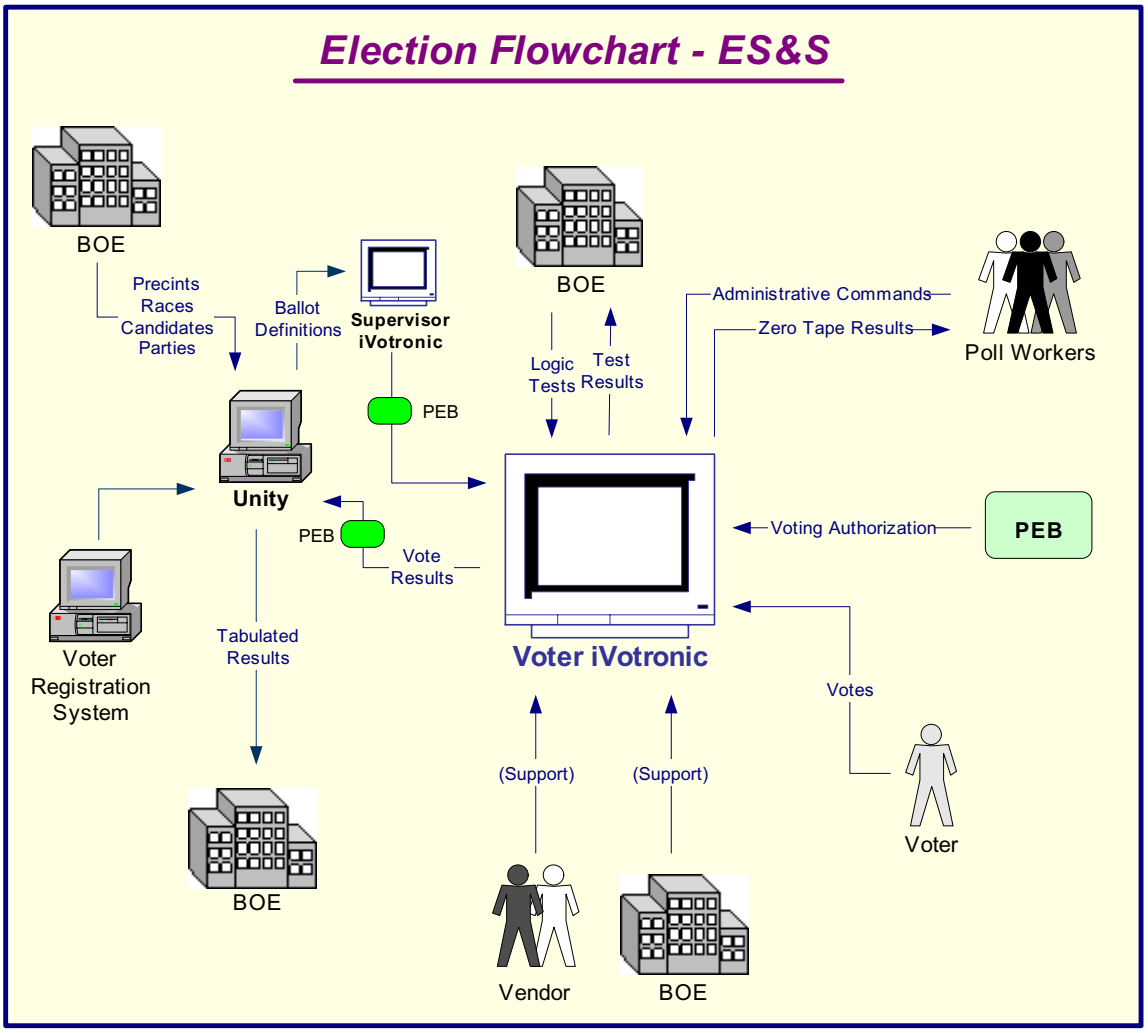

Figure 8 *– Election Flowchart - ES&S*

Continued on the next page

Work Flow/Process Model (continued)

Following is an explanation of the work flow associated with the iVotronic system interfaces.

Inputs	Outputs
Board of Elections	
• Unity Election System software is installed on a computer or on a closed network at the BOE. • Precincts are entered into the Unity Election System software either by data entry or by loading from the county voter registration system. • Races are defined in the Unity Election System software and related to the precincts. • Candidates are entered into the Unity Election System software and related to the races. • The BOE uses the Unity Election System software to create the ballot definition that is loaded to the Supervisor iVotronic and onto the Supervisor PEB. • A copy of the database is transferred to the Tally software.	
• Workers at the BOE enter data into the iVotronic to perform the logic and accuracy testing (LAT). • If there is a problem, the BOE troubleshoots the problem and determines if county workers can solve the problem or if the vendor needs to be called.	Workers at the BOE verify the results that were entered in the LAT.
Vendor	
If there are problems with the LAT, the vendor may be called in to repair the unit. If the unit is repaired, it must successfully go through the LAT tests before it may be used in an election.	
Poll Workers	
• Poll workers set up the iVotronic vote booth. • Poll workers open the iVotronic for voting using the PEB. • Poll workers authorize the voter to vote by inserting the PEB into the iVotronic unit and selecting the correct ballot for the voter.	Poll workers print a zero tape from the PEB to ensure there are no pre-existing votes recorded on it. The PEB will print reports for all iVotronics opened with the PEB.
Voter	
Voter votes the ballot. The iVotronic prevents the voter from overvoting, notifies of undervoting, and presents the ballot choices for review as appropriate.	

Continued on the next page

Work Flow/Process Model (continued)

Inputs	Outputs
Poll Workers	
	• Poll workers close all iVotronics using the same PEB that was used to open the units. • At the last iVotronic, the poll worker uses the PEB to close the unit and print result tapes. • Poll workers post one result tape at the precinct. • Poll workers remove the PEB and send the PEB and a copy of the result tape to the BOE.
Board of Elections	
	• BOE places the PEB into a Supervisor iVotronic, and the Unity Election System software reads and counts the votes. • The BOE prints and releases the results.

Environment

Hardware Configuration

Following is a summary of the hardware configuration of the ES&S iVotronic that was tested.

Processor Type	Processor Clock Speed	Memory	Operating System	Communications Slots	Input Interfaces
Intel i386 industrial	25 MHz	• 2 MB flash. Includes 3 redundant flash memories. Each are 2 MB. • Flash memory – No hard disk	Proprietary OS and firmware	• 1 (9600 bps) modem • Touchscreen, • 128MB compact flash • PEB (personal electronic ballot) proprietary device with infrared (IrDA) communica-tion	9-pin serial port for null-modem cable access

Software Configuration

Following is a summary of the software configuration of the ES&S iVotronic that was tested.

Firmware	User Interface	Internal Storage	Communications Protocols	Security
• The firmware is written in 'C'. • The source is divided into a HAL and the actual voting system.	• Uses a custom GUI interface with simple buttons and a window. • The font is Arial, and there is a minimal amount of graphics.	• No database is used internally to store data. • Data is stored in binary flat files in internal Flash Memory. • Additional fonts and audio are also stored on the Flash Memory.	• No networking is available for an iVotronic. • Uses a proprietary IrDA protocol between a PEB and the iVotronic.	• Machine stays locked until a PEB is inserted. • If a supervisor PEB is inserted, some menus become available. • Some of the supervisor menu functions are blocked by internal passwords.

Environment (continued)

Network Configuration

There is no network-based LAN\WAN connection between the DRE and the Voting Software that resides on a Windows-based machine. The only network connection that could exist is between the voting machine and central voting software. Only if the county chooses to send the accumulated votes from the polling location to the tabulating location would a dial-up connection or network connection be used.

For the scope of this project we are not reviewing any connections outside the DRE, such as dial-up connections or network connections leading to the tabulation of votes.

Step 2: Threat Identification

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. Vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised. In determining the likelihood of a threat, one must consider threat-sources, potential vulnerabilities (Step 3), and existing controls (Step 4).

In Step 2, the assessment team determined the potential threats posed to the iVotronic voting system. Following is a list of potential threats to which the iVotronic voting system could be exposed.

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Campaign and political entities	Competitive advantage Economic espionage Change outcome of election	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Step 3: Vulnerability Identification

The analysis of the threat to an electronic voting system must include an analysis of the vulnerabilities associated with the system environment. In Step 3, the assessment team identified vulnerabilities (flaws or weaknesses) of the system. Results from audits, tests, inspections, and an examination of the current state of the iVotronic voting system were used to determine existing weaknesses.

The assessment team conducted a comprehensive review of compliance to both technical and non-technical requirements to identify vulnerabilities. In addition to identifying weaknesses in the above, the team also assessed external entities and their connectivity to the iVotronic voting system.

Requirements Tested & Test Results

This section documents the requirements that were tested, the tests conducted, and the results of each test.

Test Areas

Tests were conducted in the following areas.

1. Code Review Tests
2. Platform Review Tests
3. Physical Tests

Specific Tests and Test Results

The assessment team tested the specific scenarios listed below. For each scenario, the table lists:

- Description of the requirement tested
- Test Scenario that covered the requirement
- Test Results

No.	Requirement	Test Scenario	Test Results
Code Review			
Standardization - Naming conventions of variables, constants and modules should be consistent across the application. Construction of modules within an application should also be consistent. This is important for knowledge transfer and code maintenance.			
1.01	There shall be a standard method in the naming of functions and variables.	Perform visual review of source files. Function names will be checked for proper case formatting of concatenated words. Names of functions should clearly describe its purpose.	The standardization of the code has been found to be good. The naming conventions of the variables and constants across modules are consistent and clear using good coding standards.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
Coding Conventions - The application should be broken down into modules with each module performing a single function. There should be single entry and exit points within a module. There should be consistent error handling throughout the application. Naming of variables, constants and modules should be descriptive and self-explanatory.			
1.02	There shall be standard method in the construction of modules.	Perform visual review of source files. Modules should contain a consistent format and location for module components. Modules should begin with comments describing the modules contents. Location of methods and variables with associated comments should be consistent throughout.	The modules contain descriptive file names, and descriptions of the tasks performed. The modules appear consistent file to file.
1.03	There shall be a standard methodology used for the construction of modules.	Perform visual review of source code. Modules should use a clear methodology of construction. Files will be reviewed to see if a coding industry standard is used in the naming of modules, functions, variables and constants.	The construction of the modules appears consistent across all files. No industry standard appears to be in use.
1.04	The naming of variables and functions shall be clear and descriptive.	Perform visual review of source code. Function and variable names should be "self documenting" as well as contain properly typed and sized attributes, and return types.	Variables are well named and there is appropriate use of single letter variables in loops.
1.05	There shall be a consistent way to handle system errors.	Perform visual review of source code for implementation of error handling code. All methods should contain error-handling logic. Systems should remain stable in the event of an error. When an error occurs, sufficient information regarding the state of the system and system parameters should be recorded for future debugging.	Error handling is controlled by a common class with functionality for logging.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
Code Documentation - All source code should be sufficiently commented, with clear descriptions of what is being accomplished by each module, the names of calling functions, and the inputs and outputs to the modules. Consistency should be maintained in commenting the code for ease of readability.			
1.06	The comments in the code shall be descriptive and present in the code.	Perform visual review of source code. Comments will be reviewed for simple descriptive content. Comments should appear at the beginning of each module, function. All module level variables, constants, and structures should be commented as well. Function parameters and return values should describe appropriate values. Comments should also appear in methods to help clarify complex code and logic behind expressions.	Comments are available for all of the methods of the code. Descriptions for methods and parameters are consistent in the code. Modules do have general descriptions.
1.07	The comments shall have a consistent look in their layout.	Perform visual review of source code. Comments should have a common format with standard fields for information. Some standard fields should be a description, parameters, return types, a change log.	Comments are consistent across all modules. Each module contains clearly defined areas for description, and change history.
1.08	The modules shall be commented describing their contents.	Perform visual review of source code. Modules should have a standard comment identifier at the beginning of each module. Module comments should contain the name and description of the module, a copyright notice, and a change log.	Standard comments appear at the beginning of all modules. Modules contain information in each modules header like description, change history and version. Descriptions of modules are clear and informative.
1.09	There shall be a close relationship of the requirements to the code modules that implement the requirements.	Perform visual review of the source code. Modules will be reviewed for their functional content. The variables and functions should be closely related and work directly to perform a clear task.	The modules are well structured and contain appropriately grouped functionality.
Coding Complexity - Code should be simple in construction. It should be easy to read and follow. Modules should perform single tasks and should have single points of entry and exit.			
1.10	The system shall be divided into modules.	The source code will be visually reviewed to verify if the code has been properly modularized. Modules should be an appropriate length and encapsulate related functionality.	Modules of code are well defined and grouped into appropriate areas of functionality. The use of C does not allow the use of classes.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
1.11	The source code shall use simple logic structures.	The source code will be visually reviewed for the use of simple and clear logical structures. There should be the use of constants (consts) and data structures (structs) to improve code readability and reliability.	Logic structures are clear and are an appropriate type for their use. Types and Structures have clearly defined names and internal contents are clear and grouped appropriately.
1.12	The source code shall have an appropriate size of modules and the number of functions performed by them.	The source code will be visually reviewed to verify if the code has been properly modularized. Modules should encapsulate related functionality into logical groupings with clear interfaces. Interfaces should be well defined as to their use.	Modules are of an appropriate size. Included functions are located in their correct modules. Only necessary imports are in the files.
Classes / Modules - Use of classes / modules can make the code smaller and reusable.			
1.13	There shall be the existence of classes and modules.	The source code will be visually reviewed to verify implementation of classes and proper modularization of the source files.	The code has been written in 'C' and therefore does not use classes. The files themselves are the modules of the source code and they are of an appropriate size. Internal data structures are clearly defined and well commented.
1.14	The functions performed by the classes shall be self-contained where appropriate.	The source code will be visually reviewed. The name and description of the class should be simple and clear. The task performed by the function should be easy to understand, simple to define, and atomic.	Logic inside of functions is efficient in their design. The functions have clearly defined in and out parameters.
Third Party Components - Use of third party components requires strict guidelines, security standards and version control. Attention will be paid to controls around third party components used in the applications.			
1.15	Any use of third party components in the firmware shall be inspected.	The source code will be visually reviewed to find any use of third party products. The makers and the versions of any found third party applications will be noted.	Components include drivers from Sandisk to interface with the Compact Flash slot. These have been modified to only incorporate necessary functionality.
1.16	Any third party components shall be secure and not create a risk.	If the source is available for any used third party products, the source will be reviewed for client modifications. Third party source code should only contain the necessary functionality with unused areas removed or disabled. If the source is not available then further study will be required. Source code for database access by for Crystal Reports will be reviewed.	The source has been modified to only contain necessary functionality. The IrDA drivers included for communicating with the Personal Electronic Ballot (PEB) and the iVotronic are proprietary.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
Database Review - Database integrity and data security is vital for correct data reporting. The code review will include the following:			
1.17	The database shall be well designed.	The data model and database source code will be reviewed for existence of proper keys and normalization.	There is no use of a database on the iVotronic. Data files are stored in internal and external memory as binary flat files.
1.18	The data in the database shall be secure.	The source code will be visually reviewed for user access levels and roles implemented as part of security.	Not applicable to the design of the ES&S iVotronic.
Data Integrity - Review the internal data storage of the system using the following criteria:			
1.19	There shall be ways to verify the correctness of system data.	Source code will be reviewed and tested in order to check for CRC techniques in verifying the correctness of data that is stored in memory. Can the software identify data that has been improperly modified?	The ballot data is check summed and validated when read from the PEB.
1.20	There shall not be any means by which a voter can be identified.	The source code will be reviewed to make sure that an algorithm is implemented to make sure voter records are stored in random order. The Cast Vote Records should not have time stamp associated with it.	Votes are stored in random memory buckets as each voter takes their turn. The randomness is partially seeded with the internal time clock.
1.21	The system shall be secure and prevent any access other than from authorized voters or supervisors.	The source code will be reviewed to verify the system is secure and allows each voter to only vote once by issuing unique access codes.	The PEB is keyed to an election by using an internally generated ID that is unknown to anyone using the system. At insertion the PEB is immediately disabled from anyone else using it. There are separate PEBs that only allow administrative functions, which are also password protected.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
1.22	There shall be a system to protect and backup data in the event of a disaster.	The source code will be reviewed to verify there is a means by which votes can be recovered incase of a system disaster.	The iVotronic allows for the backup and restore of a damaged iVotronic. A damaged iVotronic can be backed up onto an inserted Compact flash memory media, and copied into a new one. All transfers are logged in the internal audit data. If necessary the internal flash memory can be removed and physically transplanted into a new machine.
Encryption Standards – Review of encryption standards used in the DREs and the supporting software will be a point of primary focus while the source code is being reviewed.			
1.23	There shall be a strong method of encryption used.	The strength of encryption will be reviewed. The types of encryption will be reviewed to see if it is sufficient.	There is no use of Encryption on the iVotronic.
1.24	The data shall be encrypted including "*ballot definitions*" and other data on the DREs.	Ballot Definitions and Cast Vote Records should be protected and be verifiable they are correct. Encryption should be powerful enough to block access to stored data.	Data is not encrypted when being loaded into the iVotronic. There are safeguards with the use of a binary format and the infrared communications that prevent an unauthorized access.
1.25	There shall be the use of cryptographic operations during voter authorization.	Various means of "voter identification" should be secure. The data on a voter authorization token should not be discernable.	The PEB uses a proprietary communication protocol to identify the voter's authorization. Several checks occur including the authenticity of the PEB.
1.26	There shall be the use of encryption keys protecting types of removable media. Those keys shall be protected during the transportation of Ballot Definitions and Voting Records.	Encryption keys should be randomly generated every time and sufficiently long so that it is not easy to guess. The key its self should be kept private and not easily discovered.	The contents of the removable Compact Flash audit data are not encrypted. At the end of an election results are tallied onto PEBs.
1.27	Any data transmitted shall be encrypted over communication links.	Transmission protocols will be checked for the use on encryption. Data should never travel over a wire without protection. The contents of the transmission should be verifiable as to their contents and correctness. Any type of tampering should be identifiable if not impossible.	Transfer of results is possible via modem and their "Communications package". It was found in the software that no encryption is used during the actual transmission of the data stream. Modem protocol is Xmodem, which is CRC check summed for data transfer validation.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
1.28	The iVotronic shall not have unencrypted cast ballot records.	Check the vote records on the iVotronic and transfer medium to ensure that the records are encrypted.	There is no encryption used. All data is stored in a binary format, but only contains half of the data necessary to understand the contents.
1.29	The iVotronic shall not have unencrypted audit logs.	Check the audit logs on the iVotronic to ensure that they are encrypted.	The audit logs are not encrypted when stored on the Compact Flash card for auditing. The format is a binary format where the ASCII characters can be identified and viewed.
1.30	The system shall not store or use passwords without encryption.	Perform code review to ensure that passwords used in all software are encrypted.	Supervisor password is not encrypted and was viewable in the Compact Flash audit data.
1.31	The system shall not use hardcoded passwords.	Perform code review to ensure that the system does not use hardcoded passwords.	There are two hard coded passwords in the system. For election and system critical functions, the Supervisor password is also required. The requirement to enter a Supervisor password can be disabled using the EMS.
Platform Review			
2.01	The iVotronic shall not allow supervisor privileges to unauthorized individuals.	Attempt to convert a valid PEB into a Supervisor PEB that is recognized by the iVotronic.	No access to the PEB could be gained. The PEB is a sealed unit. It uses an infrared port to connect and will not connect to a normal Windows, Linux or Mac machine.
2.02	The system shall not allow unauthorized modification of the Ballot Definition file.	Try to modify the Ballot Definition file on the PEB before loading it on the iVotronic.	No access to the PEB could be gained. The PEB is a sealed unit. It uses an infrared port to connect and will not connect to a normal Windows, Linux or Mac machine.
2.03	The iVotronic shall not allow the installation and/or execution of an unauthorized program.	Install a program on a PEB, insert it in the iVotronic, and install and/or execute the unauthorized program.	We were unable to load a counterfeit program onto a PEB to complete this test. The PEB is a proprietary hardware interface and we could not purchase tools to assist in programming or modifying of the PEB.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
2.04	The system shall not allow for security breaches via the internet.	Inspect the iVotronic for network accessible ports.	The iVotronic contains a DB9 serial port used for connecting a printer. No other ports are available.
2.05	The system shall not allow for security breaches via the internet.	Try to access, modify, or disrupt the functioning of the iVotronic software while connected to a network.	We were not able to access or disrupt the iVotronic through the DB9 printer port.
2.06	The iVotronic shall be resistant to tampering, lock up, intrusion or vandalism.	Try to bring the system down, lock up the operating system, change or erase log files, or any other form of Denial of Service (DoS), Distributed Denial of Service (DDos), or other result which benefits the attacker.	No access could be gained. The PEB is a sealed unit. It uses an infrared port to connect and will not connect to a normal Windows, Linux or Mac machine.
2.07	The iVotronic shall not allow supervisor privileges to unauthorized individuals	Try to gain supervisor rights or system rights by any means necessary.	The only way to gain supervisor rights is by using a supervisor PEB for that specific election and by knowing the hard-coded passwords.
2.08	The operating system on the iVotronic shall be hardened against unintended intrusion, operations, or forced errors.	Try to cause a kernel panic, system failure, or indefinite wait state, or other operating system lock-up within the operating system or sub-system.	All attempts to lock the system up by using either the voter or Supervisor PEB failed. The PEB is a sealed unit. It uses an infrared port to connect and will not connect to a normal Windows, Linux or Mac machine.
2.09	The system shall password protect supervisor functions.	Observe that functions are password protected, the minimum length of passwords, and that they can be changed.	The password for the supervisor PEB is set in the Unity election management software. This can be changed for each use.
2.10	The system shall not allow corruption of the O/S, application program, ballot definition, or voter data.	Try to create an attack on flash memory using files loaded on the PEB.	Unable to load files on the PEB. The PEB is a sealed unit. It uses an infrared port to connect and will not connect to a normal Windows, Linux or Mac machine. No direct access to the iVotronic could be gained.
2.11	The system shall not allow undetected tampering with or modification to the contents of removable media.	Change the contents on a PEB and use the card. Determine if the system reports the card has been modified.	No access to the PEB could be gained. The PEB is a sealed unit. It uses an infrared port to connect and will not connect to a normal Windows, Linux or Mac machine.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
2.12	The iVotronic shall maintain a protective counter of the total number of votes cast in all elections.	Try to modify protective counter.	The protective counter is stored in non-volatile memory on the iVotronic. It cannot be modified by any supervisor or voter function including resetting the terminal.
2.13	The iVotronic shall not allow "Man-in-the-middle" attacks when communicating between the Election Management software and the iVotronic.	Observe the hardware and communication architecture to determine if network attacks are possible.	The system is not on a LAN\WAN network and the iVotronic does not dial out on a phone line in our test. The only connection to the iVotronic is the serial printer.
2.14	The iVotronic shall protect all COM ports from intrusions or vulnerabilities.	Try to gain access via an open TCP/UDP or serial or USB or other port.	The iVotronic is a sealed unit, but there are no locks in place to cover the serial port.
2.15	The iVotronic shall be resistant to introduction of Trojans, viruses, or any other form of malware.	Try to introduce any type of malicious software (malware) into the system by loading it to the PEB or compact flash card.	We were unable to load a counterfeit program onto a PEB to complete this test. The PEB is a sealed unit. It uses an infrared port to connect and will not connect to a normal Windows, Linux or Mac machine. The compact flash would not upload a malicious program into the iVotronic.
2.16	The system shall have a programmable memory device that is sealed in the unit with means of tamper detection.	Inspect the hardware design documents and physical hardware.	The iVotronic is a sealed unit, but there are no locks in place to cover the serial port. A sliding door with eyelet for a seal can be used to cover the compact flash memory card; the seal provides evidence of tampering but does not prevent access.
2.17	The system shall provide for safeguards against and evidence of tampering, theft or damage of the system and units.	Inspect the physical hardware for location of seals and locks.	The iVotronic is a sealed unit which is placed inside a voting booth. The voting booth can be closed and physically locked to prevent tampering.
2.18	In the event of the failure of a unit, the system shall retain a record of all votes cast prior to the failure.	Voted on unit, then removed power. The unit was left on overnight to drain the battery. The unit was started back up and checked for correct data.	When power was pulled or drained the memory was kept on the flash. No voting data was lost or corrupted.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
Physical Testing			
3.01	There shall be a programmable memory device sealed in unit with means of tamper detection.	The Compact Flash Card should be stored in the iVotronic with means of tamper detection.	The Compact Flash card is stored in a tamper evident unit on the iVotronic.
3.02	Poll opening reports should have all system audit information required.	Conduct logic and accuracy tests and verify system audit information is present.	Logic and accuracy tests were conducted before the election. System Audit information is present in the audit logs printed out.
3.03	The system shall store logic and accuracy test results in memory of the main unit processor and Election Day device.	Conduct Logic and Accuracy test. The results should be stored in iVotronic.	Logic and accuracy tests were conducted and stored in main memory on iVotronic. The results were printed in the audit log.
3.04	The system shall provide logic and accuracy tests in the memory of the main processor and the programmable memory device used on Election Day, including zero printouts before each election and a precinct tally printout at the close of each election.	Conduct logic and accuracy testing before election is started. Print a zero tape before an election and a result tape after an election.	Logic and accuracy tests were conducted before the election to verify counters are working properly and the programming for each voting device is correct. A zero tape printout was created and verified that no votes were cast before the start of the election. After voting was closed, a result tape was printed.
3.05	The system shall control logic and data processing methods to detect errors and provide correction method.	Create an instance where a known error will occur on the iVotronic. For instance, enter a voter card after it has been de-activated.	iVotronic displays a concise error message. This is standard throughout all error handling functions on the iVotronic.
3.06	The iVotronic shall provide a mechanism for executing test procedures which validate the correctness of election programming for each voting device and polling place and insure that the ballot display corresponds with the installed election program.	Conduct a logic and accuracy test before the start of an election.	Logic and accuracy tests were conducted before the election to verify counters are working properly and the programming for each voting device is correct.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.07	The EMS software shall not allow unauthorized modification of the Ballot Definition data.	Try to modify the Ballot Definition in the UES software using a database viewer/program.	The back end engine for the Unity software uses the popular C++ tool Codebase by Sequiter software. Codebase stores data in a dBase format which can be read and modified by Excel. Changes to data appeared in the Unity software when it was restarted.
3.08	The system shall present the ballot to the voter in a clear and unambiguous manner.	Create an election ballot definition file and transfer the file to the iVotronic. Open election on iVotronic and view a ballot.	The ballot is presented in a clear and unambiguous manner.
3.09	The iVotronic shall not allow voters to vote multiple times.	Enter a Voter PEB into the iVotronic and try to use it to vote multiple times.	Using a supervisor PEB, we can vote multiple times. Using a voter PEB, the voter can vote only once.
3.10	The iVotronic shall not allow voters to vote multiple times.	Use a counterfeit PEB in the iVotronic to vote multiple times.	Unable to duplicate the Supervisor PEB. It uses Infrared protocol with proprietary software. Windows or Linux operating systems could not recognize the Infrared. PEBs are of a proprietary design and cannot be purchased from computer vendors.
3.11	The system shall not allow voting access to unauthorized persons.	Vote without accessing a Voter PEB.	Cannot access the voting terminal without a PEB. The iVotronic doesn't power up until a PEB is placed in the PEB slot.
3.12	The iVotronic shall not allow viewing or changing vote results during the election process.	Insert a supervisor PEB in the iVotronic and try to view or change vote results.	With a supervisor PEB and three passwords we can clear a iVotronic of all votes cast. Two of the passwords are hard-coded in the firmware and are only three characters in length.
3.13	The iVotronic shall not allow the accidental or unauthorized closing of the election.	Insert a Supervisor PEB in the iVotronic and try to terminate the election early.	With a supervisor PEB and three passwords we can close an election early. Two of the passwords are hard-coded in the firmware and are only three characters in length.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.14	The iVotronic shall not allow the accidental or unauthorized reset of the iVotronic.	Insert a Supervisor PEB in the iVotronic and try to reset the iVotronic.	With a supervisor PEB and three passwords we can reset the iVotronic. Two of the passwords are hard-coded in the firmware and are only three characters in length.
3.15	The iVotronic shall not allow the use of an unauthorized PIN to access supervisor functions.	Access supervisor screens using Supervisor PEB.	With a supervisor PEB and the password to access the Service menu, we can access the Supervisor functions. The password is hard-coded in the firmware and is only three characters in length.
3.16	The iVotronic shall not lose voter information, vote count, Ballot Definition information, etc. due to a power outage during the election.	Start voting on the iVotronic, and then disconnect power for thirty minutes to simulate a power outage to iVotronic and then resume power. Cast votes before, during, and after the disruption.	The batteries were activated as soon as the power was removed and no votes were lost and the counts were accurate.
3.17	The iVotronic shall not lose voter information, vote count, Ballot Definition information, etc. due to a power outage during the election.	Start voting on the iVotronic, and then disconnect batteries for 30 minutes to simulate a power outage to iVotronic, Resume power and start up the iVotronic and check the voter information.	The batteries were removed and the iVotronic switched off. When iVotronic was turned back on, no votes cast lost and counts are accurate. PEB must be inserted again for the voter to re-start.
3.18	The iVotronic shall not allow for modification of the "protective counter" which tracks the total number of votes cast on the machine.	Try to modify the protective counter on the iVotronic.	Supervisor functions will not allow the altering of counts on the iVotronic voting machine. Counter is stored within the CPU on the iVotronic. The number on the counter is printed out before the election and after the election as well.
3.19	The iVotronic shall not allow modification that forces it to use the same storage device for all of the data.	Try to modify the iVotronic so that it unknowingly stores data and backups of data in the same location.	No access to do this operation. The iVotronic stores the data on the onboard memory. The supervisor screens do not provide the means to store data and backups of data in the same location.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.20	The system shall not allow supervisor access to unauthorized persons.	Try to access the Supervisor screen.	The iVotronic allows access to Supervisor screens with the use of a Supervisor PEB and passwords. The passwords are hard-coded in the firmware and are only three characters in length.
3.21	The audit logs shall record all instances of supervisor access to the iVotronic.	Review audit log after completing successful vote test and ensure each step that used supervisor access is correctly logged.	Each time a Supervisor PEB is used, the action is logged within the audit logs specific to the iVotronic.
3.22	The system audit log shall contain sufficient information to allow the auditing of all operations related to central site ballot tabulation, results consolidation, and report generation. It shall include a/an: • Identification of the program and version being run • Identification of the election file being used • Record of all options entered by the operator • Record of all actions performed by the subsystem • Record of all tabulation and consolidation input	Conduct an election. Print the audit log from the iVotronic and check for the required data.	Audit log was printed and all information listed in the requirement was verified.
3.23	The system audit log must be created and maintained by the system in the sequence in which operations were performed.	Review audit log after completing successful vote test and ensure each step, which used supervisor access, is correctly sequenced.	The audit log is generated in sequential order and each transaction within the audit log is time stamped.
3.24	The system audit log must be created and maintained by the system in the sequence in which operations were performed.	Conduct an election. Print the audit log from the iVotronic and check for the data to be printed in the sequence in which operations were performed.	Audit log maintained by UES software and events are listed in order of time occurred.
3.25	The system shall provide for safeguards against and evidence of tampering, theft or damage of the system and units.	Review audit logs to verify any act will be recorded and logged with a timestamp.	All actions to the iVotronic are recorded in the audit log with a time stamp. This includes opening and closing the polls, voting, inserting invalid voting cards, loss of power, and supervisor access.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.26	The media/medium in which vote counts are transferred to the Tally software shall not allow modification of the vote count.	Try to access and modify the vote count on the PEB before the vote count is loaded into the UES software.	The infrared used in the supervisor PEB could not be recognized by Windows or Linux operating systems. The company uses a proprietary protocol for transferring information using Infrared. So the tester was unable to modify the vote count on the PEB.
3.27	The system shall ensure that a voter's exact voting record cannot be traced back to the voter.	Try to access the information needed to reconstruct a voter's exact voting record.	Individual vote records are not reported from the iVotronic or tally software. The voting records are not kept in any specific order and the voter is kept anonymous. The system will provide for provisional voting by creating a sequence to list provisional voter records.
3.28	The system shall prevent modification of the voter's vote after the ballot is cast.	Attempt to change a vote, after it is cast, on the iVotronic.	We do not have access to change a vote after it has been cast. The Supervisor screen does not have any option to change the ballot after it is cast.
3.29	The system shall protect the secrecy of the vote such that the vote may not be observed during the voter's selection of preferences, during the casting of the ballot, and as the voted ballot is transmitted for recording on a storage device.	When the vote is being cast, others should not be allowed to view the voter's selection of preferences.	The secrecy of the voter is kept in place with plastic screens. Reports do not individually list votes. There are no supervisor functions to allow the viewing of an individual voter's selection.
3.30	The system shall prohibit voted ballots from being accessed by anyone until after the close of polls.	Change the votes/vote count from the iVotronic.	Ballots can only be accessed after the election is closed. Votes cannot be changed during an election. Using a Supervisor PEB and passwords, we can clear/reset the iVotronic.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.31	The system shall provide that each voter's ballot is secret and the voter cannot be identified by image, code or other methods.	Conduct a mock election and cast votes. Close the election and print out a record of each individual vote cast.	Individual vote records are not reports created from the iVotronic. The voting records are listed in no specific order and the voter is kept anonymous. Provisional voting is handled differently. Voter records can be re-constructed to verify if the vote cast is allowed or not allowed.
3.32	The system shall provide a summary screen at the end of the ballot showing what the voter has chosen prior to the final vote being cast.	Vote for all issues and/or candidates and before casting the ballot, verify a summary of all votes is presented.	A summary of all votes for each race for the particular user is displayed before we can cast the ballot. Corrections to any race can be made at this point.
3.33	The iVotronic shall not allow unauthorized modification to its operating system.	Try to modify the operating system on the iVotronic by loading a program in the PEB card.	Unable to load a program onto the PEB. The PEB card uses Infrared protocol and is not recognized by Windows or Linux Operating systems.
3.34	The iVotronic shall not allow printing of summary reports before the sequence of events required for closing of the polls are completed.	A user tries to print reports before closing the election.	The iVotronic will not allow any reports to be created or printed until the election has been closed using a Supervisor PEB.
3.35	There shall be no loss of data during generation of reports including results, images and inaccurate vote counts.	Print reports after close of an election and verify that the reports were printed correctly by matching it with the actual tally on the iVotronic.	Printed election reports after the close of the election and verified no results were lost during this function.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.36	The system shall provide printed records regarding the opening and closing of the polls and include the following: • Identification of election, including opening and closing date and times • Identification of each unit • Identification of ballot format • Identification of candidate and/or issue, verifying zero start • Identification of all ballot fields and all special voting options • Summary report of votes cast for each device, or ability to extract same	Close the election and print out a copy of the audit log and review all transactions.	Audit logs are produced on the UES software and are specific to each iVotronic. All transactions are captured on the audit logs including specific information about the iVotronic, definition of the election, and all actions occurring on the iVotronic during the election. All items identified in this requirement are present.
3.37	The system shall produce a paper audit trail. To guard against fraud, systems shall not produce individual paper records that voters could remove from the polling place.	Complete and close an election and print out a copy of the audit log from a specific iVotronic.	An audit log is printed out using a specific supervisor function. The audit log produces a report that is a paper trail to guard against fraud.
3.38	The system shall provide printout results containing candidates and/or issues in an alphanumeric format next to the vote totals.	Conduct a mock election and cast multiple votes. Once the voting is closed, print out results of the election using the supervisor functions.	Supervisor must close election and select the option to print votes cast. The printout presents the votes cast in a summary format.
3.39	The system shall allow for extraction of data from memory devices to a central host.	The PEB should contain the totals for the iVotronic, which can be transferred to the central host.	Supervisor PEB (which contains the totals of the iVotronic) is transferred to UES software, with no problems.
3.40	The Tally software shall not allow double counting of votes from a precinct or iVotronic.	Upload election results from an iVotronic to the tally software. Upload them a second time.	Results can be added multiple times due to a feature that gives an option to either add or replace the votes when uploading the results into the Unity Election System (UES) software. The system will allow an iVotronic to be double-posted.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.41	The Tally software shall not allow modification of the vote count.	Try to modify the vote tally in the UES software using a tool such as MS Excel or MS Access.	The Tally software stores data in a set of ISAM file structures. These data structures are not ODBC compliant and could not be accessed from MS Excel.
3.42	The system shall provide for summary reports of votes cast on each voting device by extracting information from a memory device or a removable data storage device.	Conduct an election. Cast votes. Close the election. Print summary reports from iVotronic.	Supervisor must close election and select the option to print votes cast. This can only be done when election has been closed. Once all iVotronic voting machines have closed all results are uploaded to UES where reports are created. Reports can be created to show results for each iVotronic.
3.43	The system shall provide for easily downloading results from balloting into the final tally of votes.	Conduct a mock election and have multiple voters cast ballots. Once the election is closed, the transferring of votes to UES software for tallying and reporting is done.	The supervisor must access these functions using a supervisor PEB. The supervisor PEB then uploads all results of the vote from each iVotronic voting machine. Voting tallies for each iVotronic are transferred to the UES software to produce reports.
3.44	The system shall accurately report all votes cast.	Set up a mock election and cast multiple votes. Verify all votes have been included in reports created by UES.	All votes have been included in counts recorded by UES software. All reports in UES accurately reflect number of votes cast on iVotronic.
3.45	The system shall provide a cumulative, canvass and precinct report of absentee voting, provisional ballot voting and Election Day voting as one total.	Verify election management software has the ability to handle provisional and absentee ballot voting.	Verified that functionality for recording absentee and provisional voting exists in the UES software.
3.46	The system shall provide a cumulative, canvass and precinct report of Election Day Voting as one total.	Complete an election. Print the reports from the Host computer.	Printed the reports from the UES software. Verified that provisional voting and absentee ballots were included.
3.47	The system shall not lose votes, corrupt media or have performance issues due to the presence of a magnetic field.	A magnet is placed on the LCD unit on the iVotronic and the PEB slot when voting.	There was no visible degradation on the display. During voting, the magnetic field did not affect the iVotronic and no votes were lost.

Step 4: Controls Analysis

The Secretary of State has not been required to have a security plan in place for electronic voting systems in the past. As a result of HAVA, the requirement now exists.

Based on the findings of this report and the report developed by InfoSENTRY, the Secretary of State will develop a new security plan or modify the existing security plan to include risk mitigation strategies to minimize or eliminate the likelihood of threat.

Step 5: Threat Likelihood

In Step 5, the assessment team examined the threats identified in Step 2 against each potential vulnerability, and assigned a likelihood rating. The likelihood rating indicates the probability that a potential vulnerability may be exercised, taking into account the nature of the threat, motivation and capability of the threat-source (if human), and existence and effectiveness of current controls.

Each potential vulnerability was assigned a threat likelihood rating of High, Medium, or Low. The following table lists the potential vulnerabilities identified and their likelihood rating.

Potential Vulnerability Identified	Threat Likelihood Rating
Hacking	Low
System intrusion, break-ins -Physical	Medium
Unauthorized system access- Physical	Medium
Fraudulent act	Low
Information bribery	Low
Spoofing	Low
System intrusion	Low
Bomb/Terrorism	Low
Information warfare	Low
System attack	Low
System penetration	Medium
System tampering	Medium
Economic exploitation	Low
Information theft	Low
Intrusion on personal privacy	Low
Unauthorized system access (access to classified, proprietary, and/or technology-related information)	Low
Unauthorized system access	Low
System sabotage	Low
System bugs	Low
Malicious code	Low
Fraud and theft	Low
Input of falsified, corrupted data	Low
Interception	Low

Step 6: Impact Analysis

In Step 6, the assessment team determined the adverse impact(s) that would likely occur if a threat-source were able to successfully exploit a vulnerability or weakness. The team followed the process below to determine the adverse impact resulting from a successful exploitation of a vulnerability:

- Determined the criticality of the electronic voting system and data to accomplishing the SOS' mission.
- Determined the probable adverse impact of a successful exploitation of a vulnerability.
- Determined the adverse impact of a security event in regard to loss or degradation of the system's integrity, availability, and confidentiality.
- Assigned a rating of High, Medium, or Low to each vulnerability to indicate the magnitude of impact resulting from a successful exploitation of the vulnerability.

The following table shows the magnitude of impact rating that was assigned to each potential vulnerability.

Potential Vulnerability Identified	Magnitude of Impact Rating
Code Review	
Encryption: No published encryption methodology is used in the system to protect the ballot information, cast vote records, audit logs, passwords and during data transmission.	Low
Platform Review	
PEB - If someone had access to the Supervisor PEB, they could gain access to the system.	High
Password - the default password is generic from ES&S on the PEB.	Medium
Locks - With access someone could steal the flash memory card if one was present. There are no covers or locks to secure the flash memory if it was being used.	Medium
Physical Testing	
Supervisor PEB can be used to vote multiple times.	High
iVotronic has passwords hard-coded into the firmware.	High
UES Software has the ability of double counting of votes from PEB.	High

Step 7: Determine Risks

The purpose of Step 7 is to assess the level of risk to the electronic voting system. In this step, the assessment team identified the risk(s), if any, arising out of each test scenario. After identifying the risks, the team assigned a risk rating for each vulnerability by combining the results of the Impact Analysis established in Step 6 with the Likelihood of Threat established in Step 5. The combination of the impact analysis and the threat likelihood versus the security controls in place were applied to a risk-level matrix to determine the resultant risk-level.

Risks Identified

The assessment team identified the following vulnerabilities of the iVotronic voting system. For each vulnerability identified, the table lists the relevant requirement tested, test scenario, and test results which identified the vulnerability.

No.	Test Scenario	Test Result	Risk Identified
Code Review			
1.01	Perform visual review of source files. Function names will be checked for proper case formatting of concatenated words. Names of functions should clearly describe its purpose.	The standardization of the code has been found to be good. The naming conventions of the variables and constants across modules are consistent and clear using good coding standards.	None.
1.02	Perform visual review of source files. Modules should contain a consistent format and location for module components. Modules should begin with comments describing the modules contents. Location of methods and variables with associated comments should be consistent throughout.	The modules contain descriptive file names, and descriptions of the tasks performed. The modules appear consistent file to file.	None.
1.03	Perform visual review of source code. Modules should use a clear methodology of construction. Files will be reviewed to see if a coding industry standard is used in the naming of modules, functions, variables and constants.	The construction of the modules appears consistent across all files. No coding industry standard appears to be in use.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.04	Perform visual review of source code. Function and variable names should be "self documenting" as well as contain properly typed and sized attributes, and return types.	Variables are well named and there is appropriate use of single letter variables in loops.	None.
1.05	Perform visual review of source code for implementation of error handling code. All methods should contain error-handling logic. Systems should remain stable in the event of an error. When an error occurs, sufficient information regarding the state of the system and system parameters should be recorded for future debugging.	Error handling is controlled by a common class with functionality for logging.	None.
1.06	Perform visual review of source code. Comments will be reviewed for simple descriptive content. Comments should appear at the beginning of each module, function. All module level variables, constants, and structures should be commented as well. Function parameters and return values should describe appropriate values. Comments should also appear in methods to help clarify complex code and logic behind expressions.	Comments are available for all of the methods of the code. Descriptions for methods and parameters are consistent in the code. Modules do have general descriptions.	None.
1.07	Perform visual review of source code. Comments should have a common format with standard fields for information. Some standard fields should be a description, parameters, return types, a change log.	Comments are consistent across all modules. Each module contains clearly defined areas for description, and change history.	None.
1.08	Perform visual review of source code. Modules should have a standard comment identifier at the beginning of each module. Module comments should contain the name and description of the module, a copyright notice, and a change log.	Standard comments appear at the beginning of all modules. Modules contain information in each modules header like description, change history and version. Descriptions of modules are clear and informative.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.09	Perform visual review of the source code. Modules will be reviewed for their functional content. The variables and functions should be closely related and work directly to perform a clear task.	The modules are well structured and contain appropriately grouped functionality.	None.
1.10	The source code will be visually reviewed to verify if the code has been properly modularized. Modules should be an appropriate length and encapsulate related functionality.	Modules of code are well defined and grouped into appropriate areas of functionality. The use of C does not allow the use of classes.	None.
1.11	The source code will be visually reviewed for the use of simple and clear logical structures. There should be the use of constants (consts) and data structures (structs) to improve code readability and reliability.	Logic structures are clear and are an appropriate type for their use. Types and Structures have clearly defined names and internal contents are clear and grouped appropriately.	None.
1.12	The source code will be visually reviewed to verify if the code has been properly modularized. Modules should encapsulate related functionality into logical groupings with clear interfaces. Interfaces should be well defined as to their use.	Modules are of an appropriate size. Included functions are located in their correct modules. Only necessary imports are in the files.	None.
1.13	The source code will be visually reviewed to verify implementation of classes and proper modularization of the source files.	The code has been written in ‘C’ and therefore does not use classes. The files themselves are the modules of the source code and they are of an appropriate size. Internal data structures are clearly defined and well commented.	None.
1.14	The source code will be visually reviewed. The name and description of the class should be simple and clear. The task performed by the function should be easy to understand, simple to define, and atomic.	Logic inside of functions is efficient in their design. The functions have clearly defined in and out parameters.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.15	The source code will be visually reviewed to find any use of third party products. The makers and the versions of any found third party applications will be noted.	Components include drivers from Sandisk to interface with the Compact Flash slot. These have been modified to only incorporate necessary functionality.	None.
1.16	If the source is available for any used third party products, the source will be reviewed for client modifications. Third party source code should only contain the necessary functionality with unused areas removed or disabled. If the source is not available then further study will be required. Source code for database access by for Crystal Reports will be reviewed.	The source has been modified to only contain necessary functionality. The IrDA drivers included for communicating with the PEB and the iVotronic are proprietary.	None.
1.17	The data model and database source code will be reviewed for existence of proper keys and normalization.	There is no use of a database on the iVotronic. Data files are stored in internal and external memory as binary flat files.	None.
1.18	The source code will be visually reviewed for user access levels and roles implemented as part of security.	Not applicable to the design of the ES&S iVotronic.	None.
1.19	Source code will be reviewed and tested in order to check for CRC techniques in verifying the correctness of data that is stored in memory. Can the software identify data that has been improperly modified?	The ballot data is check summed and validated when read from the PEB.	None.
1.20	The source code will be reviewed to make sure that an algorithm is implemented to make sure voter records are stored in random order. The Cast Vote Records should not have time stamp associated with it.	Votes are stored in random memory buckets as each voter takes their turn. The randomness is partially seeded with the internal time clock.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.21	The source code will be reviewed to verify the system is secure and allows each voter to only vote once by issuing unique access codes.	The PEB is keyed to an election by using an internally generated ID that is unknown to anyone using the system. At insertion the PEB is immediately disabled from anyone else using it. There are separate PEBs that only allow administrative functions, which are also password protected.	None.
1.22	The source code will be reviewed to verify there is a means by which votes can be recovered incase of a system disaster.	The iVotronic allows for the backup and restore of a damaged DRE. A damaged iVotronic can be backed up onto an inserted Compact flash memory media, and copied into a new one. All transfers are logged in the internal audit data. If necessary the internal flash memory can be removed and physically transplanted into a new machine.	None.
1.23	The strength of encryption will be reviewed. The types of encryption will be reviewed to see if it is sufficient.	There is no use of Encryption on the iVotronic.	There is no use of Encryption on the iVotronic or on data transferred to and from the iVotronic. There is a risk that an unauthorized person could gain access to the data.
1.24	Ballot Definitions and Cast Vote Records should be protected and be verifiable they are correct. Encryption should be powerful enough to block access to stored data.	Data is not encrypted when being loaded into the iVotronic. There are safeguards with the use of a binary format and the infrared communications that prevent an unauthorized access.	There is no use of Encryption on the iVotronic or on data transferred to and from the iVotronic. There is a risk that an unauthorized person could access ballot definitions and/or cast vote records on the iVotronic or on the PEB.
1.25	Various means of "voter identification" should be secure. The data on a voter authorization token should not be discernable.	The PEB uses a proprietary communication protocol to identify the voter's authorization. Several checks occur including the authenticity of the PEB.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.26	Encryption keys should be randomly generated every time and sufficiently long so that it is not easy to guess. The key its self should be kept private and not easily discovered.	The contents of the removable Compact Flash audit data are not encrypted. At the end of an election results are tallied onto PEBs.	Same as 1.24 - There is no use of Encryption on the iVotronic or on data transferred to and from the iVotronic. There is a risk that an unauthorized person could access ballot definitions and/or cast vote records on the iVotronic or on the PEB.
1.27	Transmission protocols will be checked for the use on encryption. Data should never travel over a wire without protection. The contents of the transmission should be verifiable as to their contents and correctness. Any type of tampering should be identifiable if not impossible.	Transfer of results is possible via modem and their "Communications package". It was found in the software that no encryption is used during the actual transmission of the data stream. Modem protocol is Xmodem, which is CRC check summed for data transfer validation.	Transfer of election results is possible via modem and the ES&S "Communications package". No encryption is used during the actual transmission of the data stream. There is a risk that an unauthorized person could intercept and view election data.
1.28	Check the vote records on the iVotronic and transfer medium to ensure that the records are encrypted.	There is no encryption used. All data is stored in a binary format, but only contains half of the data necessary to understand the contents.	Same as 1.24 - There is no use of Encryption on the iVotronic or on data transferred to and from the iVotronic. There is a risk that an unauthorized person could access ballot definitions and/or cast vote records on the iVotronic or on the PEB.
1.29	Check the audit logs on the iVotronic to ensure that they are encrypted.	The audit logs are not encrypted when stored on the Compact Flash card for auditing. The format is a binary format where the ASCII characters can be identified and viewed.	The audit logs are not encrypted when stored on the Compact Flash card. This card is removable. There is a risk that an unauthorized person could view or modify audit logs stored in the Compact Flash card.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.30	Perform code review to ensure that passwords used in all software are encrypted.	Supervisor password is not encrypted and was viewable in the Compact Flash audit data.	The iVotronic uses a physical device (PEB) plus two hardcoded passwords to limit access to supervisory functions. There is a risk that an unauthorized person with knowledge of these passwords might access supervisory functions on the iVotronic.
1.31	Perform code review to ensure that the system does not use hardcoded passwords.	There are two hard coded passwords in the system. For election and system critical functions, the Supervisor password is also required. The requirement to enter a Supervisor password can be disabled using the EMS.	a) Same as 1.30 – The iVotronic uses a physical device (PEB) plus two hardcoded passwords to limit access to supervisory functions. There is a risk that an unauthorized person with knowledge of these passwords might access supervisory functions on the iVotronic. b) One user-set supervisor password is available to protect selected iVotronic functions. We can choose to disable this password when the election is setup on the election management software. There is a risk that due to the disabling of the supervisor password, an unauthorized person might access supervisory functions on the iVotronic.
Platform Review			
2.01	Attempt to convert a valid PEB into a Supervisor PEB that is recognized by the iVotronic.	No access to the PEB could be gained. The PEB is a sealed unit. It uses an infrared port to connect and will not connect to a normal Windows, Linux or Mac machine.	None.
2.02	Try to modify the Ballot Definition file on the PEB before loading it on the iVotronic.	No access to the PEB could be gained. The PEB is a sealed unit. It uses an infrared port to connect and will not connect to a normal Windows, Linux or Mac machine.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
2.03	Install a program on a PEB, insert it in the iVotronic, and install and/or execute the unauthorized program.	We were unable to load a counterfeit program onto a PEB to complete this test. The PEB is a proprietary hardware interface and we could not purchase tools to assist in programming or modifying of the PEB.	None.
2.04	Inspect the iVotronic for network accessible ports.	The iVotronic contains a DB9 serial port used for connecting a printer. No other ports are available.	None.
2.05	Try to access, modify, or disrupt the functioning of the iVotronic software while connected to a network.	We were not able to access or disrupt the iVotronic through the DB9 printer port.	None.
2.06	Try to bring the system down, lock up the operating system, change or erase log files, or any other form of Denial of Service (DoS), Distributed Denial of Service (DDos), or other result which benefits the attacker.	No access could be gained. The PEB is a sealed unit. It uses an infrared port to connect and will not connect to a normal Windows, Linux or Mac machine.	None.
2.07	Try to gain supervisor rights or system rights by any means necessary.	The only way to gain supervisor rights is by using a supervisor PEB for that specific election and by knowing the hard-coded passwords.	The iVotronic uses a physical device (PEB) plus two hardcoded passwords to limit access to supervisory functions. There is a risk that an unauthorized person with access to the Supervisor PEB and knowledge of the hard-coded passwords might gain access to supervisory functions on the system.
2.08	Try to cause a kernel panic, system failure, or indefinite wait state, or other operating system lock-up within the operating system or sub-system.	All attempts to lock the system up by using either the voter or Supervisor PEB failed. The PEB is a sealed unit. It uses an infrared port to connect and will not connect to a normal Windows, Linux or Mac machine.	None.
2.09	Observe that functions are password protected, the minimum length of passwords, and that they can be changed.	The password for the supervisor PEB is set in the Unity election management software. This can be changed for each use.	There is a risk that an unauthorized person can gain access to the preset Supervisor password.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
2.10	Try to create an attack on flash memory using files loaded on the PEB.	Unable to load files on the PEB. The PEB is a sealed unit. It uses an infrared port to connect and will not connect to a normal Windows, Linux or Mac machine. No direct access to the iVotronic could be gained.	None.
2.11	Change the contents on a PEB and use the card. Determine if the system reports the card has been modified.	No access to the PEB could be gained. The PEB is a sealed unit. It uses an infrared port to connect and will not connect to a normal Windows, Linux or Mac machine.	None.
2.12	Try to modify protective counter.	The protective counter is stored in non-volatile memory on the iVotronic. It cannot be modified by any supervisor or voter function including resetting the terminal.	None.
2.13	Observe the hardware and communication architecture to determine if network attacks are possible.	The system is not on a LAN\WAN network and the iVotronic does not dial out on a phone line in our test. The only connection to the iVotronic is the serial printer.	None.
2.14	Try to gain access via an open TCP/UDP or serial or USB or other port.	The iVotronic is a sealed unit, but there are no locks in place to cover the serial port.	None.
2.15	Try to introduce any type of malicious software (malware) into the system by loading it to the PEB or compact flash card.	We were unable to load a counterfeit program onto a PEB to complete this test. The PEB is a sealed unit. It uses an infrared port to connect and will not connect to a normal Windows, Linux or Mac machine. The compact flash would not upload a malicious program into the iVotronic.	None.
2.16	Inspect the hardware design documents and physical hardware.	The iVotronic is a sealed unit, but there are no locks in place to cover the serial port. A sliding door with eyelet for a seal can be used to cover the compact flash memory card; the seal provides evidence of tampering but does not prevent access.	There is a risk that the Compact Flash card can be removed by an unauthorized person during an election if the Compact flash card compartment is not sealed.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
2.17	Inspect the physical hardware for location of seals and locks.	The iVotronic is a sealed unit which is placed inside a voting booth. The voting booth can be closed and physically locked to prevent tampering.	None.
2.18	Voted on unit, then removed power. The unit was left on overnight to drain the battery. The unit was started back up and checked for correct data.	When power was pulled or drained the memory was kept on the flash. No voting data was lost or corrupted.	None.
Physical Testing			
3.01	The Compact Flash Card should be stored in the iVotronic with means of tamper detection.	The Compact Flash card is stored in a tamper evident unit on the iVotronic.	Same as 2.16 - There is a risk that the Compact Flash card can be removed by an unauthorized person during an election if the Compact flash card compartment is not sealed.
3.02	Conduct logic and accuracy tests and verify system audit information is present.	Logic and accuracy tests were conducted before the election. System Audit information is present in the audit logs printed out.	None.
3.03	Conduct Logic and Accuracy test. The results should be stored in iVotronic.	Logic and accuracy tests were conducted and stored in main memory on iVotronic. The results were printed in the audit log.	None.
3.04	Conduct logic and accuracy testing before election is started. Print a zero tape before an election and a result tape after an election.	Logic and accuracy tests were conducted before the election to verify counters are working properly and the programming for each voting device is correct. A zero tape printout was created and verified that no votes were cast before the start of the election. After voting was closed, a result tape was printed.	None.
3.05	Create an instance where a known error will occur on the iVotronic. For instance, enter a voter card after it has been de-activated.	iVotronic displays a concise error message. This is standard throughout all error handling functions on the iVotronic.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.06	Conduct a logic and accuracy test before the start of an election.	Logic and accuracy tests were conducted before the election to verify counters are working properly and the programming for each voting device is correct.	None.
3.07	Try to modify the Ballot Definition in the UES software using a database viewer/program.	The back end engine for the Unity software uses the popular C++ tool Codebase by Sequiter software. Codebase stores data in a dBase format which can be read and modified by Excel. Changes to data appeared in the Unity software when it was restarted.	There is a risk that an unauthorized person with access to the Unity server and a loaded viewer program might modify the ballot definitions stored in the database.
3.08	Create an election ballot definition file and transfer the file to the DRE. Open election on DRE and view a ballot.	The ballot is presented in a clear and unambiguous manner.	None.
3.09	Enter a Voter PEB into the DRE and try to use it to vote multiple times.	Using a supervisor PEB, we can vote multiple times. Using a voter PEB, the voter can vote only once.	A poll worker can initiate voting on the iVotronic using just the Supervisor PEB. There is a risk that an unauthorized person with access to a supervisor PEB could cast multiple ballots.
3.10	Use a counterfeit PEB in the DRE to vote multiple times.	Unable to duplicate the Supervisor PEB. It uses Infrared protocol with proprietary software. Windows or Linux operating systems could not recognize the Infrared. PEBs are of a proprietary design and cannot be purchased from computer vendors.	None.
3.11	Vote without accessing a Voter PEB.	Cannot access the voting terminal without a PEB. The DRE doesn't power up until a PEB is placed in the PEB slot.	None.
3.12	Insert a supervisor PEB in the iVotronic and try to view or change vote results.	With a supervisor PEB and three passwords we can clear an iVotronic of all votes cast. Two of the passwords are hard-coded in the firmware and are only three characters in length.	With a supervisor PEB and three passwords we can clear an iVotronic of all votes cast. Two of the passwords are hard-coded in the firmware and are only three characters in length. There is a risk that an unauthorized person could view or clear vote results if the person has access to all passwords and supervisor PEB's.

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.13	Insert a Supervisor PEB in the iVotronic and try to terminate the election early.	With a supervisor PEB and three passwords we can close an election early. Two of the passwords are hard-coded in the firmware and are only three characters in length.	With a supervisor PEB and two passwords we can close the polls on an iVotronic. One of the passwords is hard-coded in the firmware and only three characters in length. There is a risk that an unauthorized person could terminate an election early if the person has access to passwords and supervisor PEB's.
3.14	Insert a Supervisor PEB in the iVotronic and try to reset the iVotronic.	With a supervisor PEB and three passwords we can reset the iVotronic. Two of the passwords are hard-coded in the firmware and are only three characters in length.	With a supervisor PEB and three passwords we can reset an iVotronic. Two of the passwords are hard-coded in the firmware and are only three characters in length. There is a risk that an unauthorized user could reset the iVotronic if the person has access to all passwords and supervisor PEB's.
3.15	Access supervisor screens using Supervisor PEB.	With a supervisor PEB and the password to access the Service menu, we can access the Supervisor functions. The password is hard-coded in the firmware and is only three characters in length.	With a supervisor PEB and three passwords we can access any supervisory functions. Two of the passwords are hard-coded in the firmware and are only three characters in length. There is a risk that an unauthorized user could access the Supervisor functions if the person had access to the Service menu password and supervisor PEB.
3.16	Start voting on the iVotronic, and then disconnect power for thirty minutes to simulate a power outage to iVotronic and then resume power. Cast votes before, during, and after the disruption.	The batteries were activated as soon as the power was removed and no votes were lost and the counts were accurate.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.17	Start voting on the iVotronic, and then disconnect batteries for 30 minutes to simulate a power outage to iVotronic, Resume power and start up the iVotronic and check the voter information.	The batteries were removed and the iVotronic switched off. When iVotronic was turned back on, no votes cast lost and counts are accurate. PEB must be inserted again for the voter to re-start.	None.
3.18	Try to modify the protective counter on the iVotronic.	Supervisor functions will not allow the altering of counts on the iVotronic. Counter is stored within the CPU on the iVotronic. The number on the counter is printed out before the election and after the election as well.	None.
3.19	Try to modify the iVotronic so that it unknowingly stores data and backups of data in the same location.	No access to do this operation. The iVotronic stores the data on the onboard memory. The supervisor screens do not provide the means to store data and backups of data in the same location.	None.
3.20	Try to access the Supervisor screen.	The iVotronic allows access to Supervisor screens with the use of a Supervisor PEB and passwords. The passwords are hard-coded in the firmware and are only three characters in length.	With a supervisor PEB and three passwords we can access any supervisory function on the iVotronic. Two of the passwords are hard-coded in the firmware and are only three characters in length. There is a risk that an unauthorized person could access the Supervisor screen if the person has access to all passwords and supervisor PEB's.
3.21	Review audit log after completing successful vote test and ensure each step that used supervisor access is correctly logged.	Each time a Supervisor PEB is used, the action is logged within the audit logs specific to the iVotronic.	None.
3.22	Conduct an election. Print the audit log from the iVotronic and check for the required data.	Audit log was printed and all information listed in the requirement was verified.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.23	Review audit log after completing successful vote test and ensure each step, which used supervisor access, is correctly sequenced.	The audit log is generated in sequential order and each transaction within the audit log is time stamped.	None.
3.24	Conduct an election. Print the audit log from the iVotronic and check for the data to be printed in the sequence in which operations were performed.	Audit log maintained by UES software and events are listed in order of time occurred.	None.
3.25	Review audit logs to verify any act will be recorded and logged with a timestamp.	All actions to the iVotronic are recorded in the audit log with a time stamp. This includes opening and closing the polls, voting, inserting invalid voting cards, loss of power, and supervisor access.	None.
3.26	Try to access and modify the vote count on the PEB before the vote count is loaded into the UES software.	The infrared used in the supervisor PEB could not be recognized by Windows or Linux operating systems. The company uses a proprietary protocol for transferring information using Infrared. So the tester was unable to modify the vote count on the PEB.	None.
3.27	Try to access the information needed to reconstruct a voter's exact voting record.	Individual vote records are not reported from the iVotronic or tally software. The voting records are not kept in any specific order and the voter is kept anonymous. The system will provide for provisional voting by creating a sequence to list provisional voter records.	None.
3.28	Attempt to change a vote, after it is cast, on the iVotronic.	We do not have access to change a vote after it has been cast. The Supervisor screen does not have any option to change the ballot after it is cast.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.29	When the vote is being cast, others should not be allowed to view the voter's selection of preferences.	The secrecy of the voter is kept in place with plastic screens. Reports do not individually list votes. There are no supervisor functions to allow the viewing of an individual voter's selection.	None.
3.30	Change the votes/vote count from the iVotronic.	Ballots can only be accessed after the election is closed. Votes cannot be changed during an election. Using a Supervisor PEB and passwords, we can clear/reset the iVotronic.	None.
3.31	Conduct a mock election and cast votes. Close the election and print out a record of each individual vote cast.	Individual vote records are not reports created from the iVotronic. The voting records are listed in no specific order and the voter is kept anonymous. Provisional voting is handled differently. Voter records can be re-constructed to verify if the vote cast is allowed or not allowed.	None.
3.32	Vote for all issues and/or candidates and before casting the ballot, verify a summary of all votes is presented.	A summary of all votes for each race for the particular user is displayed before we can cast the ballot. Corrections to any race can be made at this point.	None.
3.33	Try to modify the operating system on the iVotronic by loading a program in the PEB card.	Unable to load a program onto the PEB. The PEB card uses Infrared protocol and is not recognized by Windows or Linux Operating systems.	None.
3.34	A user tries to print reports before closing the election.	The iVotronic will not allow any reports to be created or printed until the election has been closed using a Supervisor PEB.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.35	Print reports after close of an election and verify that the reports were printed correctly by matching it with the actual tally on the iVotronic.	Printed election reports after the close of the election and verified no results were lost during this function.	None.
3.36	Close the election and print out a copy of the audit log and review all transactions.	Audit logs are produced on the UES software and are specific to each iVotronic. All transactions are captured on the audit logs including specific information about the iVotronic, definition of the election, and all actions occurring on the iVotronic during the election. All items identified in this requirement are present.	None.
3.37	Complete and close an election and print out a copy of the audit log from a specific iVotronic.	An audit log is printed out using a specific supervisor function. The audit log produces a report that is a paper trail to guard against fraud.	None.
3.38	Conduct a mock election and cast multiple votes. Once the voting is closed, print out results of the election using the supervisor functions.	Supervisor must close election and select the option to print votes cast. The printout presents the votes cast in a summary format.	None.
3.39	The PEB should contain the totals for the iVotronic, which can be transferred to the central host.	Supervisor PEB (which contains the totals of the iVotronic) is transferred to UES software, with no problems.	None.
3.40	Upload election results from a iVotronic to the tally software. Upload them a second time.	Results can be added multiple times due to a feature that gives an option to either add or replace the votes when uploading the results into the UES software. The system will allow an iVotronic to be double-posted.	The ES&S tally program has an "Add To" feature intended to collect data from a broken machine. This function can be executed multiple times for the same DRE with no warning, which results in overcounting of these votes. There is a risk that the election results for an iVotronic might be uploaded to the Unity Election System (UES) software multiple times, and as a result votes would be overcounted.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.41	Try to modify the vote tally in the UES software using a tool such as MS Excel or MS Access.	The Tally software stores data in a set of ISAM file structures. These data structures are not ODBC compliant and could not be accessed from MS Excel.	None.
3.42	Conduct an election. Cast votes. Close the election. Print summary reports from iVotronic.	Supervisor must close election and select the option to print votes cast. This can only be done when election has been closed. Once all iVotronic voting machines have closed all results are uploaded to UES where reports are created. Reports can be created to show results for each iVotronic.	None.
3.43	Conduct a mock election and have multiple voters cast ballots. Once the election is closed, the transferring of votes to UES software for tallying and reporting is done.	The supervisor must access these functions using a supervisor PEB. The supervisor PEB then uploads all results of the vote from each iVotronic voting machine. Voting tallies for each iVotronic are transferred to the UES software to produce reports.	None.
3.44	Set up a mock election and cast multiple votes. Verify all votes have been included in reports created by UES.	All votes have been included in counts recorded by UES software. All reports in UES accurately reflect number of votes cast on iVotronic.	None.
3.45	Verify election management software has the ability to handle provisional and absentee ballot voting.	Verified that functionality for recording absentee and provisional voting exists in the UES software.	None.
3.46	Complete an election. Print the reports from the Host computer.	Printed the reports from the UES software. Verified that provisional voting and absentee ballots were included.	None.
3.47	A magnet is placed on the LCD unit on the iVotronic and the PEB slot when voting.	There was no visible degradation on the display. During voting, the magnetic field did not affect the iVotronic and no votes were lost.	None.

Risk Levels of Identified Risks

Each Threat-Source/Vulnerability was assigned a rating of High, Medium, or Low to represent the degree or level of risk to which the electronic voting system might be exposed if a given vulnerability were exercised. Following is a description of the High, Medium, and Low ratings.

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, it must determined whether corrective actions are still required or whether the risk can be accepted.

The following table shows the rating assigned to each identified risk.

No.	Risk Identified	Risk Likelihood	Impact Rating	Risk Level
Code Review				
1.23	There is no use of Encryption on the iVotronic or on data transferred to and from the iVotronic. There is a risk that an unauthorized person could gain access to the data.	Low	Low	Low
1.24 1.26 1.28	There is no use of Encryption on the iVotronic or on data transferred to and from the iVotronic. There is a risk that an unauthorized person could access ballot definitions and/or cast vote records on the iVotronic or on the PEB.	Low	Low	Low
1.27	Transfer of election results is possible via modem and the ES&S "Communications package". No encryption is used during the actual transmission of the data stream. There is a risk that an unauthorized person could intercept and view election data.	Low	Medium	Low

Continued on the next page

Risk Levels of Identified Risks (continued)

No.	Risk Identified	Risk Likelihood	Impact Rating	Risk Level
1.29	The audit logs are not encrypted when stored on the Compact Flash card. This card is removable. There is a risk that an unauthorized person could view or modify audit logs stored in the Compact Flash card.	Low	Low	Low
1.30 1.31(a)	The iVotronic uses a physical device (PEB) plus two hardcoded passwords to limit access to supervisory functions. There is a risk that an unauthorized person with knowledge of these passwords might access supervisory functions on the iVotronic.	Medium	High	Medium
1.31(b)	One user-set supervisor password is available to protect selected iVotronic functions. We can choose to disable this password when the election is setup on the election management software. There is a risk that due to the disabling of the supervisor password, an unauthorized person might access supervisory functions on the iVotronic.	Medium	High	Medium
Platform Review				
2.07	The iVotronic uses a physical device (PEB) plus two hardcoded passwords to limit access to supervisory functions. There is a risk that an unauthorized person with access to the Supervisor PEB and knowledge of the hard-coded passwords might gain access to supervisory functions on the system.	Low	High	Low
2.09	There is a risk that an unauthorized person can gain access to the preset Supervisor password.	Low	High	Low
2.16	There is a risk that the Compact Flash card can be removed by an unauthorized person during an election if the Compact flash card compartment is not sealed.	Low	Low	Low
Physical Testing				
3.01	Same as 2.16 above.			
3.07	There is a risk that an unauthorized person with access to the Unity server and a loaded viewer program might modify the ballot definitions stored in the database.	Low	High	Low

Continued on the next page

Risk Levels of Identified Risks (continued)

No.	Risk Identified	Risk Likelihood	Impact Rating	Risk Level
3.09	A poll worker can initiate voting on the iVotronic using just the Supervisor PEB. There is a risk that an unauthorized person with access to a supervisor PEB could cast multiple ballots.	Medium	High	Medium
3.12	With a supervisor PEB and three passwords we can clear an iVotronic of all votes cast. Two of the passwords are hard-coded in the firmware and are only three characters in length. There is a risk that an unauthorized person could view or clear vote results if the person has access to all passwords and supervisor PEB's.	Low	High	Low
3.13	With a supervisor PEB and two passwords we can close the polls on an iVotronic. One of the passwords is hard-coded in the firmware and only three characters in length. There is a risk that an unauthorized person could terminate an election early if the person has access to passwords and supervisor PEB's.	Low	High	Low
3.14	With a supervisor PEB and three passwords we can reset a iVotronic. Two of the passwords are hard-coded in the firmware and are only three characters in length. There is a risk that an unauthorized user could reset the iVotronic if the person has access to all passwords and supervisor PEB's.	Low	High	Low
3.15	With a supervisor PEB and three passwords we can access any supervisory functions. Two of the passwords are hard-coded in the firmware and are only three characters in length. There is a risk that an unauthorized user could access the Supervisor functions if the person had access to the Service menu password and supervisor PEB.	Low	High	Low
3.20	With a supervisor PEB and three passwords we can access any supervisory function on the iVotronic. Two of the passwords are hard-coded in the firmware and are only three characters in length. There is a risk that an unauthorized person could access the Supervisor screen if the person has access to all passwords and supervisor PEB's.	Low	High	Low
3.40	The ES&S tally program has an "Add To" feature intended to collect data from a broken machine. This function can be executed multiple times for the same DRE with no warning, which results in overcounting of these votes. There is a risk that the election results for an iVotronic DRE might be uploaded to the UES software multiple times, and as a result votes would be overcounted.	High	High	High

Step 8: Risk Mitigation Strategies

In Step 8, the assessment team recommended solutions that are intended to mitigate or eliminate the risks identified in Step 7. The goal of the recommended risk mitigation strategies is to reduce the level of risk to the electronic voting system and its data to an acceptable level.

Recommended Risk Mitigation Strategies

The assessment team recommends the following mitigation strategies for the risks identified during this assessment.

Code Review

No.	Risk Identified	Recommended Mitigation Strategy
High Risk		
	N/A	
Medium Risk		
1.30 1.31(a)	The iVotronic uses a physical device (PEB) plus two hardcoded passwords to limit access to supervisory functions. There is a risk that an unauthorized person with knowledge of these passwords might access supervisory functions on the iVotronic.	We recommend the Secretary of State require that ES&S incorporate user-changeable passwords of at least six characters in length. We also recommend the Secretary of State require that administrative policies and procedures be put into place regarding password management.
1.31(b)	One user-set supervisor password is available to protect selected iVotronic functions. We can choose to disable this password when the election is setup on the election management software. There is a risk that due to the disabling of the supervisor password, an unauthorized person might access supervisory functions on the iVotronic.	We recommend the Secretary of State require that ES&S incorporate user-changeable passwords of at least six characters in length. We also recommend the Secretary of State require that administrative policies and procedures be put into place regarding password management.
Low Risk		
1.23	There is no use of Encryption on the iVotronic or on data transferred to and from the iVotronic. There is a risk that an unauthorized person could gain access to the data.	We recommend the Secretary of State require that ES&S incorporate strong encryption to protect data.
1.24 1.26 1.28	There is no use of Encryption on the iVotronic or on data transferred to and from the iVotronic. There is a risk that an unauthorized person could access ballot definitions and/or cast vote records on the iVotronic or on the PEB.	We recommend the Secretary of State require that ES&S incorporate strong encryption to protect data.

Continued on the next page

Recommended Risk Mitigation Strategies (continued)

Code Review (continued)

No.	Risk Identified	Recommended Mitigation Strategy
1.27	Transfer of election results is possible via modem and the ES&S "Communications package". No encryption is used during the actual transmission of the data stream. There is a risk that an unauthorized person could intercept and view election data.	We recommend the Secretary of State require that ES&S incorporate strong encryption to protect data.
1.29	The audit logs are not encrypted when stored on the Compact Flash card. This card is removable. There is a risk that an unauthorized person could view or modify audit logs stored in the Compact Flash card.	We recommend the Secretary of State require that ES&S incorporate strong encryption to protect data.

Platform Review

No.	Risk Identified	Recommended Mitigation Strategy
High Risk		
	N/A	
Medium Risk		
	N/A	

Continued on the next page

Recommended Risk Mitigation Strategies (continued)

Platform Review (continued)

No.	Risk Identified	Recommended Mitigation Strategy
Low Risk		
2.07	The iVotronic uses a physical device (PEB) plus two hardcoded passwords to limit access to supervisory functions. There is a risk that an unauthorized person with access to the Supervisor PEB and knowledge of the hard-coded passwords might gain access to supervisory functions on the system.	We recommend the Secretary of State require that administrative policies and procedures be put into place regarding password management and physical security of the PEBs. We also recommend the Secretary of State require that ES&S incorporate user-changeable passwords of at least six characters in length.
2.09	There is a risk that an unauthorized person can gain access to the preset Supervisor password.	We recommend the Secretary of State require that ES&S incorporate user-changeable passwords of at least six characters in length. We also recommend the Secretary of State require that administrative policies and procedures be put into place regarding password management.
2.16	There is a risk that the Compact Flash card can be removed by an unauthorized person during an election if the Compact flash card compartment is not sealed.	We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk.

Physical Testing

No.	Risk Identified	Recommended Mitigation Strategy
High Risk		
3.40	The ES&S tally program has an "Add To" feature intended to collect data from a broken machine. This function can be executed multiple times for the same DRE with no warning, which results in overcounting of these votes. There is a risk that the election results for an iVotronic DRE might be uploaded to the UES software multiple times, and as a result votes would be overcounted..	We recommend the Secretary of State require that ES&S modify the software to prevent duplicate counting of votes. We also recommend the Secretary of State require that administrative policies and procedures be put into place regarding use of the "Add To" feature.

Continued on the next page

Recommended Risk Mitigation Strategies (continued)

Physical Testing (continued)

No.	Risk Identified	Recommended Mitigation Strategy
Medium Risk		
3.09	A poll worker can initiate voting on the iVotronic using just the Supervisor PEB. There is a risk that an unauthorized person with access to a supervisor PEB could cast multiple ballots.	We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk.
Low Risk		
3.01	Same as 2.16 under Platform Review section above.	Same as 2.16 under Platform Review section above.
3.07	There is a risk that an unauthorized person with access to the Unity server and a loaded viewer program might modify the ballot definitions stored in the database.	We recommend the Secretary of State require that administrative policies and procedures be put into place to require use of proper Windows login security on the EMS server and to prevent unauthorized access, and not contain any additional software that would allow access to the EMS database.
3.12	With a supervisor PEB and three passwords we can clear an iVotronic of all votes cast. Two of the passwords are hard-coded in the firmware and are only three characters in length. There is a risk that an unauthorized person could view or clear vote results if the person has access to all passwords and supervisor PEB's.	We recommend the Secretary of State require that ES&S incorporate user-changeable passwords of at least six characters in length. We also recommend the Secretary of State require that administrative policies and procedures be put into place regarding password management and physical security of the PEB.
3.13	With a supervisor PEB and two passwords we can close the polls on an iVotronic. One of the passwords is hard-coded in the firmware and only three characters in length. There is a risk that an unauthorized person could terminate an election early if the person has access to passwords and supervisor PEB's.	We recommend the Secretary of State require that ES&S incorporate user-changeable passwords of at least six characters in length. We also recommend the Secretary of State require that administrative policies and procedures be put into place regarding password management and physical security of the PEB.

Continued on the next page

Recommended Risk Mitigation Strategies (continued)

Physical Testing (continued)

No.	Risk Identified	Recommended Mitigation Strategy
3.14	With a supervisor PEB and three passwords we can reset an iVotronic. Two of the passwords are hard-coded in the firmware and are only three characters in length. There is a risk that an unauthorized user could reset the iVotronic if the person has access to all passwords and supervisor PEB's.	We recommend the Secretary of State require that ES&S incorporate user-changeable passwords of at least six characters in length. We also recommend the Secretary of State require that administrative policies and procedures be put into place regarding password management and physical security of the PEB.
3.15	With a supervisor PEB and three passwords we can access any supervisory functions. Two of the passwords are hard-coded in the firmware and are only three characters in length. There is a risk that an unauthorized user could access the Supervisor functions if the person had access to the Service menu password and supervisor PEB.	We recommend the Secretary of State require that ES&S incorporate user-changeable passwords of at least six characters in length. We also recommend the Secretary of State require that administrative policies and procedures be put into place regarding password management and physical security of the PEB.
3.20	With a supervisor PEB and three passwords we can access any supervisory function on the iVotronic. Two of the passwords are hard-coded in the firmware and are only three characters in length. There is a risk that an unauthorized person could access the Supervisor screen if the person has access to all passwords and supervisor PEB's.	We recommend the Secretary of State require that ES&S incorporate user-changeable passwords of at least six characters in length. We also recommend the Secretary of State require that administrative policies and procedures be put into place regarding password management and physical security of the PEBs.

Step 9: Document Results

In Step 9, the assessment team combined the results of Steps 1 through 8 to develop this report detailing the technical security assessment and its findings.

Conclusion

Compuware has conducted a study of the ES&S iVotronic voting system to identify specific security vulnerabilities that might be exploited during an election and to recommend actions to mitigate these vulnerabilities. The scope of this study has been limited to reviewing the technical implementation of the iVotronic and reviewing each data stream into and from the iVotronic. It has not included a review of the policies, procedures, or work practices of either ES&S or the Ohio Secretary of State.

During the course of our study, Compuware has identified several significant security issues, which left unmitigated would provide an opportunity for an attacker to disrupt the election process or throw the election results into question. These are documented above. Following careful consideration of each of these security issues, we have developed mitigation recommendations for the Secretary of State to implement which we believe will limit the likelihood of a successful attack on the election process. Provided each of these mitigation recommendations can be enacted, Compuware has concluded the ES&S iVotronic can be securely deployed by the Secretary of State.

Although all risks documented above must be dealt with appropriately, the most significant risk areas, which will require the most effort to mitigate, include:

Risk Identified	Recommended Mitigation Strategy
ES&S does not use encryption to protect election data transferred to and from the iVotronic. There is a risk that an unauthorized person could gain access to election data.	We recommend the Secretary of State require that ES&S incorporate strong encryption to protect data.
ES&S has hardcoded some supervisory passwords. If an attacker with knowledge of these passwords can access a PEB configured for the current election, they can execute supervisory functions including casting unauthorized votes and closing the polls early. There is a risk that an unauthorized person with knowledge of the supervisory passwords and access to a Supervisor PEB could cast multiple ballots.	We recommend the Secretary of State require that ES&S incorporate user-changeable passwords of at least six characters in length. We also recommend the Secretary of State require that administrative policies and procedures be put into place regarding password management and physical security of the Supervisor PEBs.
The Unity election management software allows the user to perform an “ADD TO” function, which adds results from a DRE to a precinct’s totals. This function does not detect when a DRE is added more than once resulting in incorrect vote tallies. There is a risk that the election results for a DRE can be uploaded to the UES software multiple times, and the votes would be counted multiple times.	We recommend the Secretary of State require that ES&S modify the software to prevent duplicate counting of votes.

Election policies and procedures have long been used to ensure fair and accurate election results. The deployment of DRE technology will not lessen the need for well thought out and consistently enforced policies and procedures.

This page intentionally left blank.

PART FOUR: HART INTERCIVIC

Overview

This section details the assessment for the Hart InterCivic eSlate 3000 DRE. The eSlate 3000 is a fully-featured electronic voting system with an integrated mechanical selector, and has a flexible ballot presentation and polycarbonate screen. The unit is ADA accessible by design, and can be upgraded to provide additional accessibility.

Judge's Booth Controllers (JBCs) are used to manage the election process in the precinct and to issue access codes for the voters. The system uses a Mobile Ballot Box (MBB) feature in which the eSlate's PCMCIA flash memory card is the storage medium for all voting information to operate the eSlate system.

The Ballot Origination Software System (BOSS) enables users to define and create ballot styles for all precincts. Election data is written to MBBs and will configure every product of the eSlate system in any location. The Tally software tallies votes, and provides standard reports and a custom report writer for producing customized reports.

The eSlate 3000 prevents the voter from overvoting, notifies the voter of undervoting, and allows the voter to review and modify their ballot choices before casting their vote. .

Compuware tested the following hardware and software in this technical security assessment:

Hardware	Software
• eSlate 3000 version 2.1 • Judge's Booth Controller (JBC) version 1.16	• BOSS Election Management Software version 2.9.04 • TALLY software version 2.9.08 • SERVO software version 1.0.2

Step 1: Characterization of the eSlate 3000 Voting System

In Step 1, the eSlate 3000 was examined for the following:

- eSlate 3000 system interfaces – input/output connections between the eSlate 3000 and external entities, and the related voting processes
- Work flow / process model – flow of data through the eSlate 3000 system interfaces, and the related voting processes
- eSlate 3000 environment
    - Hardware configuration
    - Software configuration
    - Network configuration

eSlate 3000 System Interfaces

The following diagram provides a graphical overview of the connections to the eSlate 3000. The diagram shows the input/output connections between the eSlate 3000 and external entities such as the BOE's and voters.

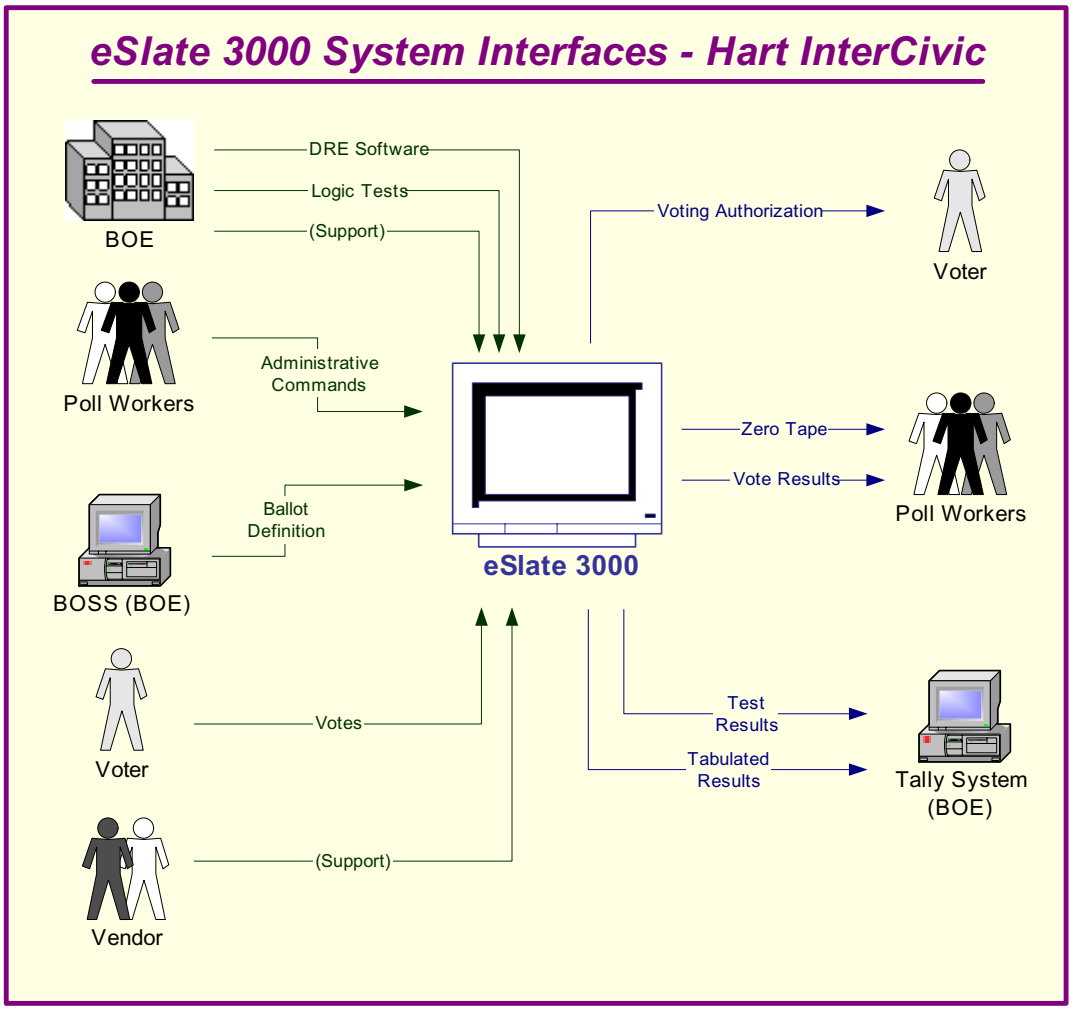

Figure 9 – *eSlate 3000 System Interfaces - Hart InterCivic*

Continued on the next page

eSlate 3000 System Interfaces (continued)

Following is an explanation of the tasks related to the eSlate 3000 system interfaces.

Inputs	Outputs
Board of Elections	
• The BOSS Election Management Software is installed on a computer at the Board of Elections (BOE). • The BOE uses the BOSS Software to create the ballot definition that is loaded to the Judge's Booth Controller (JBC).	
• Workers at the BOE enter data into the eSlate to perform the logic and accuracy testing (LAT). • If there is a problem, the BOE troubleshoots the problem and determines if county workers can solve the problem or if the vendor needs to be called.	Workers at the board verify the results that were entered in the LAT.
Vendor	
If there is a problem with the LAT, the vendor may be called in to repair the unit. If the unit is repaired, it must successfully go through the LAT before it may be used in an election.	
Poll Workers	
• Poll workers set up the booth. • Poll workers open the eSlates for voting. • Poll workers authorize the voter to vote.	Poll workers print a zero tape from the JBC to ensure there are no pre-existing votes recorded on the unit.
Voter	
• Voter takes the authorization to the eSlate, which presents the correct ballot for the voter. • Voter votes the ballot. The eSlate prevents the voter from overvoting, notifies of undervoting, and presents the ballot choices for review as appropriate.	
Poll Workers	
	• Poll workers print result tapes from the JBC. • Poll workers post one result tape at the precinct. • Poll workers remove the PCMCIA media and send the media and a copy of the result tape to the BOE.
Board of Elections	
	• The BOE places the PCMCIA media from the JBC into a media reader, and the Tally software counts the votes. • The BOE prints and releases the results.

Work Flow / Process Model

The following diagram provides a graphical overview of the work flow associated with the eSlate 3000 system interfaces, and represents the next level down from the Context Diagram. This diagram displays the flow of data through the eSlate 3000 system interfaces.

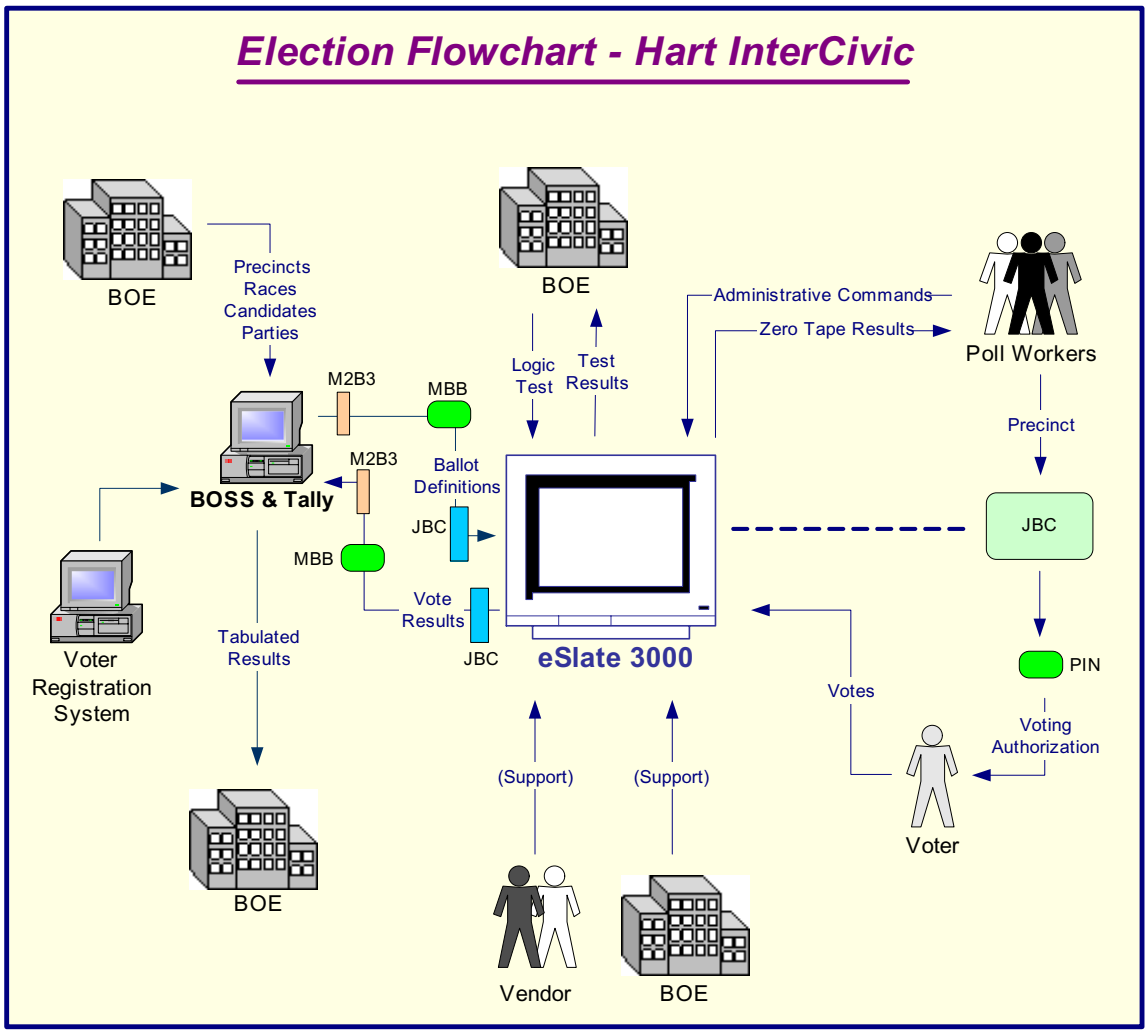

Figure 10 *– Election Flowchart - Hart InterCivic*

Continued on the next page

Work Flow / Process Model (continued)

Following is an explanation of the work flow associated with the eSlate 3000 system interfaces.

Inputs	Outputs
Board of Elections	
• The BOSS Election Management Software is installed on a computer or on a closed network at the BOE. • Precincts are entered into the BOSS Election Management Software either by data entry or by loading from the county voter registration system. • Races are defined in the BOSS Election Management Software and related to the precincts. • Candidates are entered into the BOSS Election Management Software and related to the races. • The BOE uses the BOSS Election Management Software to create the ballot definition on a PCMCIA card that then becomes the Mobile Ballot Box (MBB). • The MBB is loaded into the Judge's Booth Controller (JBC). • A copy of the database is transferred to the Tally software to be used to count the results.	
• Workers at the BOE enter data into the eSlate to perform the logic and accuracy testing (LAT). • If there is a problem, the BOE troubleshoots the problem and determines if county workers can solve the problem or if the vendor needs to be called.	Workers at the BOE verify the results that were entered in the LAT.
Vendor	
If there is a problem with the LAT, the vendor may be called in to repair the unit. If the unit is repaired, it must successfully go through the LAT before it may be used in an election.	
Poll Workers	
• Poll workers set up the eSlate vote booth. • Poll workers open the JBC for voting. • Poll workers authorize the voter to vote and the JBC assigns a PIN to the voter. This PIN is given to the voter.	Poll workers print a zero tape from the JBC to ensure there are no pre-existing votes recorded on it.
Voter	
• Voter enters the PIN into the eSlate, which then displays the correct ballot for the voter. • Voter votes the ballot. The eSlate prevents the voter from overvoting, notifies of undervoting, and presents the ballot choices for review as appropriate.	

Continued on the next page

Work Flow/Process Model (continued)

Inputs	Outputs
Poll Workers	
	• Poll workers print the result tapes from the JBC. • Poll workers post one result tape at the precinct. • Poll workers remove the MBB and send the MBB and a copy of the result tape to the BOE.
Board of Elections	
	• BOE places the MBB from the JBC into a media reader, and the Tally software counts the votes. • The BOE prints and releases the results.

Environment

Hardware Configuration

Following is a summary of the hardware configuration of the Hart InterCivic eSlate 3000 that was tested.

Processor Type	Processor Clock Speed	Memory	Operating System	Communications Slots	Input Interfaces
Motorola Coldfire 5307	90 MHz	• 4 MB flash memory. • There are 3 separate memory locations: PCMCIA, eSlate (2 chips), JBC (4 chips) • 128 MB compact flash card – No hard disk	Precise MQX RTOS (real-time operating system) 32-bits	• Stripped down (subset) of RS485, 1MB	Serial RS-485, compact flash

Software Configuration

Following is a summary of the software configuration of the Hart InterCivic eSlate 3000 that was tested.

Firmware	User Interface	Internal Storage	Communications Protocols	Security
Precise MQX RTOS (real-time operating system) 32-bits	Proprietary GUI software displayed on an LCD allowing user input through push buttons and wheel.	The data is stored in binary format in the PC card in Mobile Ballot Box, Judge's Booth Controller and eSlate devices.	• Stripped down version of RS485, 1MB.	• Voters can access eSlate device using the access code generated by the JBC. • JBC can be set up to have password access.

Environment (continued)

Network Configuration

There is no network-based LAN\WAN connection between the DRE and the Voting Software that resides on a Windows-based machine. The only network connection that could exist is between the voting machine and central voting software. Only if the county chooses to send the accumulated votes from the polling location to the tabulating location would a dial-up connection or network connection be used.

For the scope of this project we are not reviewing any connections outside the DRE, such as dial-up connections or network connections leading to the tabulation of votes.

Step 2: Threat Identification

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. Vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised. In determining the likelihood of a threat, one must consider threat-sources, potential vulnerabilities (Step 3), and existing controls (Step 4).

In Step 2, the assessment team determined the potential threats posed to the eSlate 3000 voting system. Following is a list of potential threats to which the eSlate 3000 voting system could be exposed.

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Campaign and political entities	Competitive advantage Economic espionage Change outcome of election	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Step 3: Vulnerability Identification

The analysis of the threat to an electronic voting system must include an analysis of the vulnerabilities associated with the system environment. In Step 3, the assessment team identified vulnerabilities (flaws or weaknesses) of the system. Results from audits, tests, inspections, and an examination of the current state of the eSlate 3000 voting system were used to determine existing weaknesses.

The assessment team conducted a comprehensive review of compliance to both technical and non-technical requirements to identify vulnerabilities. In addition to identifying weaknesses in the above, the team also assessed external entities and their connectivity to the eSlate 3000 voting system.

Requirements Tested & Test Results

This section documents the requirements that were tested, the tests conducted, and the results of each test.

Test Areas

Tests were conducted in the following areas.

1. Code Review Tests
2. Platform Review Tests
3. Physical Tests

Specific Tests and Test Results

The assessment team tested the specific scenarios listed below. For each scenario, the table lists:

- Description of the requirement tested
- Test Scenario that covered the requirement
- Test Results

No.	Requirement	Test Scenario	Test Results
Code Review			
Standardization - Naming conventions of variables, constants and modules should be consistent across the application. Construction of modules within an application should also be consistent. This is important for knowledge transfer and code maintenance.			
1.01	There shall be a standard method in the naming functions and variables.	Perform visual review of source files. Function names will be checked for proper case formatting of concatenated words. Names of functions should clearly describe its purpose.	The function names are in proper and consistent case format and the names describe the high level purpose of the function.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
1.02	There shall be standard method in the construction of modules.	Perform visual review of source files. Modules should contain a consistent format and location for module components. Modules should begin with comments describing the modules contents. Location of methods and variables with associated comments should be consistent throughout.	Modules are consistent with respect to the format of comments and location of methods and variables.
Coding Conventions - The application should be broken down into modules with each module performing a single function. There should be single entry and exit points within a module. There should be consistent error handling throughout the application. Naming of variables, constants and modules should be descriptive and self-explanatory.			
1.03	There shall be a standard methodology used for the construction of modules.	Perform visual review of source code. Modules should use a clear methodology of construction. Files will be reviewed to see if a coding industry standard is used in the naming of modules, functions, variables and constants.	Module construction appears to be consistent throughout the source code. The code uses a consistent naming standard.
1.04	The naming of variables and functions shall be clear and descriptive.	Perform visual review of source code. Function and variable names should be "self documenting" as well as contain properly typed and sized attributes, and return types.	The function and variable names describe their purpose. Proper attribute and return types are used in the code. Library descriptions are very informative.
1.05	There shall be a consistent way to handle system errors.	Perform visual review of source code for implementation of error handling code. All methods should contain error-handling logic. Systems should remain stable in the event of an error. When an error occurs, sufficient information regarding the state of the system and system parameters should be recorded for future debugging.	Review of the code indicates that error-handling code has been implemented. Error-handling code returns clear messages to the users in the event of errors. There are safeguards to prevent the system from crashing. The error and audit log entries are tracked in the eSlate.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
Code Documentation - All source code should be sufficiently commented, with clear descriptions of what is being accomplished by each module, the names of calling functions, and the inputs and outputs to the modules. Consistency should be maintained in commenting the code for ease of readability.			
1.06	The comments in the code shall be descriptive and present in the code.	Perform visual review of source code. Comments will be reviewed for simple descriptive content. Comments should appear at the beginning of each module, function. All module level variables, constants, and structures should be commented as well. Function parameters and return values should describe appropriate values. Comments should also appear in methods to help clarify complex code and logic behind expressions.	Comments are present at the beginning of modules and briefly describe their purpose. Functions and methods contain comments describing their purpose. Module level variables, constants and structures are commented, and those that are not commented have self-describing names to identify their purpose.
1.07	The comments shall have a consistent look in their layout.	Perform visual review of source code. Comments should have a common format with standard fields for information. Some standard fields should be a description, parameters, return types, a change log.	The comments are in a common format containing entries including change log and describing function and module purpose.
1.08	The modules shall be commented describing their contents.	Perform visual review of source code. Modules should have a standard comment identifier at the beginning of each module. Module comments should contain the name and description of the module, a copyright notice, and a change log.	Module comments contain name, description, and a detailed change log. Copyright information is also available at the beginning of modules.
1.09	There shall be a close relationship of the requirements to the code modules that implement the requirements.	Perform visual review of the source code. Modules will be reviewed for their functional content. The variables and functions should be closely related and work directly to perform a clear task.	Modules perform clearly specified tasks. Unused variables and functions were not found in the code.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
Coding Complexity - Code should be simple in construction. It should be easy to read and follow. Modules should perform single tasks and should have single points of entry and exit.			
1.10	The system shall be divided into modules.	The source code will be visually reviewed to verify if the code has been properly modularized. Modules should be an appropriate length and encapsulate related functionality.	Several modules have been created based on functionality and code is reused in the system. The modules are of reasonable length.
1.11	The source code shall use simple logic structures.	The source code will be visually reviewed for the use of simple and clear logical structures. There should be the use of constants and structures to improve code readability and reliability.	Constants (consts) and data structures (structs) are used wherever necessary in the code to improve readability and reliability.
1.12	The source code shall have an appropriate size of modules and the number of functions performed by them.	The source code will be visually reviewed to verify if the code has been properly modularized. Modules should encapsulate related functionality into logical groupings with clear interfaces. Interfaces should be well defined as to their use.	The code is properly modularized and the module size is managed correctly by implementing necessary functionality.
Classes / Modules - Use of classes / modules can make the code smaller and reusable.			
1.13	There shall be the existence of classes and modules.	The source code will be visually reviewed to verify implementation of classes and proper modularization of the source files.	Most of the MBB creation utility and PVS code is written in C. C does not implement classes, so they have not been used. But proper modularization of code is done.
1.14	The functions performed by the classes shall be self-contained where appropriate.	The source code will be visually reviewed. The name and description of the class should be simple and clear. The task performed by the function should be easy to understand, simple to define, and atomic.	The code has many modules and each implements specific functionality. The module size is appropriate and the code is readable and easy to understand.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
Third Party Components - Use of third party components requires strict guidelines, security standards and version control. Attention will be paid to controls around third party components used in the applications.			
1.15	Any use of third party components in the firmware shall be inspected.	The source code will be visually reviewed to find any use of third party products. The makers and the versions of any found third party applications will be noted.	The eSlate and JBC uses an Mqx 2.4 Operating System. The source code for this operating system is currently owned and maintained by Hart InterCivic.
1.16	Any third party components shall be secure and not create a risk.	If the source is available for any used third party products, the source will be reviewed for client modifications. Third party source code should only contain the necessary functionality with unused areas removed or disabled. If the source is not available then further study will be required.	The source code only contains the necessary functionality for the JBC and eSlate units. Other in-house developed utilities are also packaged with the Mqx operating system.
Database Review – Database integrity and data security is vital for correct data reporting. The code review will include the following:			
1.17	The database shall be well designed.	The data model and database source code will be reviewed for existence of proper keys and normalization.	The eSlate does not use a database. Data files are stored in internal and external memory (MBB) in binary format. The Boss and Tally applications use a common SQLAnywhere database. The data dictionary did not indicate primary keys.
1.18	The data in the database shall be secure.	The source code will be visually reviewed for user access levels and roles implemented as part of security.	Not applicable to the design of Hart InterCivic eSlate.
Data Integrity - Review the internal data storage of the system using the following criteria:			
1.19	There shall be ways to verify the correctness of system data.	Source code will be reviewed and tested in order to check for CRC techniques in verifying the correctness of data that is stored in memory. Can the software identify data that has been improperly modified?	CRC 16 algorithm has been implemented in the code. CRC checks are performed every time data is written to the MBB or internal memory of eSlate machines and Judge's Booth Controller. The checks are also done when data is transmitted from each eSlate to the JBC unit.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
1.20	There shall not be any means by which a voter can be identified.	The source code will be reviewed to make sure that an algorithm is implemented to make sure voter records are stored in random order. The Cast Vote Records should not have time stamp associated with it.	The vote records are stored randomly in the storage media (MBB, internal memory of eSlate and JBC). An appropriate algorithm is implemented in the code to store the data randomly and without time stamp.
1.21	The system shall be secure and prevent any access other than from authorized voters or supervisors.	The source code will be reviewed to verify the system is secure and allows each voter to only vote once by issuing unique access codes.	The source code for JBC generates unique access codes for a precinct. Voters use these codes to access the eSlate device and cast their votes. These access codes are valid only for a specified time (which is set in the BOSS system) and eSlate device does not accept these codes after that time has expired.
1.22	There shall be a system to protect and backup data in the event of a disaster.	The source code will be reviewed to verify there is a means by which votes can be recovered incase of a system disaster.	Vote and audit information is stored in 3 places – MBB, internal memory in eSlate, and JBC. In the event of a disaster, the SERVO software can re-create MBBs with data from either the JBC or eSlate devices. System alerts are given in case of errors during data transmission between eSlate units and JBC.
Encryption Standards - Review of encryption standards used in the DREs and the supporting software will be a point of primary focus while the source code is being reviewed.			
1.23	There shall be a strong method of encryption used.	The strength of encryption will be reviewed. The types of encryption will be reviewed to see if it is sufficient.	No published encryption methodology is used in the system.
1.24	The data shall be encrypted including "*ballot definitions*" and other data on the DREs.	Ballot Definitions and Cast Vote Records should be protected and be verifiable they are correct. Encryption should be powerful enough to block access to stored data.	Code is not available to encrypt ballot definition and cast vote records in the eSlate. But the data is stored in proprietary binary format.
1.25	There shall be the use of cryptographic operations during voter authorization.	Various means of "voter identification" should be secure. The data on a voter authorization token should not be discernable.	The voter is identified to the eSlate based on a four-digit PIN generated by the JBC. Based on code review, the voter information is not stored anywhere in the system.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
1.26	There shall be the use of encryption keys protecting types of removable media. Those keys shall be protected during the transportation of Ballot Definitions and Voting Records.	Encryption keys should be randomly generated every time and sufficiently long so that it is not easy to guess. The key itself should be kept private and not easily discovered.	No published encryption methodology is used in the system.
1.27	Any data transmitted shall be encrypted over communication links.	Transmission protocols will be checked for the use on encryption. Data should never travel over a wire without protection. The contents of the transmission should be verifiable as to their contents and correctness. Any type of tampering should be identifiable if not impossible.	Communication between JBC and eSlate units uses RS485 protocol. The data transmitted between these units is not encrypted. After the polls are closed, the MBBs or eSlate units are physically transported to the computer(s) at a central location and are read by the Tally or SERVO software to tally the results.
1.28	The eSlate shall not have unencrypted cast ballot records.	Check the vote records on the Mobile Ballot Box, Ballot Origination Software, Tally and Servo software, and transfer medium to ensure that the records are encrypted.	No published encryption methodology is used in the system.
1.29	The eSlate shall not have unencrypted audit logs.	Check the audit logs on the PVS to ensure that they are encrypted.	No published encryption methodology was found to store audit log information.
1.30	The system shall not store or use passwords without encryption.	Perform code review to ensure that passwords used in all software are encrypted.	No published encryption methodology is used in the system to protect the passwords.
1.31	The system shall not use hardcoded passwords.	Perform code review to ensure that the system does not use hardcoded passwords.	Hardcoded passwords are not used in the system.
Platform Review			
2.01	The eSlate shall not allow supervisor privileges to unauthorized individuals.	Attempt to gain access to the system in supervisor mode.	There is not a supervisor mode on the Hart eSlate.
2.02	The system shall not allow unauthorized modification of the Ballot Definition file.	Try to modify the Ballot Definition file on the MBB card before loading it on the eSlate.	The MBB is on a linear card and could not be read by the Windows file system. We were unable to modify the ballot definition file while it was on the MBB.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
2.03	The eSlate shall not allow the installation and/or execution of an unauthorized program.	Install a program on a MBB card, insert it in the eSlate, and install and/or execute the unauthorized program.	The MBB is on a linear card and could not be read by the Windows file system. We were unable to place a counterfeit program on the MBB.
2.04	The system shall not allow for security breaches via the internet.	Inspect the eSlate for network accessible ports.	The eSlate has two serial ports used to connect to the eSlate on either side of the daisy chain. The JBC has three serial ports. One is used for a 9600 baud modem connection. One goes to the first eSlate, and one goes to a printer. The ports that are on the eSlate could not be used for network communication.
2.05	The system shall not allow for security breaches via the internet.	Try to access, modify, or disrupt the functioning of the JBC or eSlate software while connected to a network.	The JBC cannot be connected to a network. A modem port is present but has been disabled in this version.
2.06	The eSlate shall be resistant to tampering, lock up, intrusion or vandalism.	Try to bring the system down, lock up the operating system, change or erase log files, or any other form of Denial of Service (DoS), Distributed Denial of Service (DDos), or other result which benefits the attacker.	Attempts to disrupt the JBC using the ports on the machine were unsuccessful due to limitations of the proprietary operating system.
2.07	The eSlate shall not allow supervisor privileges to unauthorized individuals.	Try to gain supervisor rights or system rights by any means necessary.	There are no supervisor modes on the JBC or eSlate. Access to supervisor function is limited by physical access to the JBC.
2.08	The operating system on the eSlate shall be hardened against unintended intrusion, operations, or forced errors.	Try to cause a kernel panic, system failure, or indefinite wait state, or other operating system lock-up within the operating system or sub-system.	The MBB is on a linear card and could not be read by the Windows file system. No access could be gained to the eSlate or the JBC to try to bring the system down. Attempts to access ports on the machines were unsuccessful due to the proprietary operating system.
2.09	The system shall password protect supervisor functions.	Observe that functions are password protected, the minimum length of passwords, and that they can be changed.	The password can be changed within the BOSS software. The minimum length of the password is zero.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
2.10	The system shall not allow corruption of the O/S, application program, ballot definition, or voter data.	Try to create an attack on flash memory using files loaded on the MBB card.	The MBB is on a linear card and could not be read by the Windows file system.
2.11	The system shall not allow undetected tampering with or modification to the contents of removable media.	Change the contents on a removable media card and use the card. Determine if the system reports the card has been modified.	The MBB is on a linear card and could not be read by the Windows file system.
2.12	The eSlate shall maintain a protective counter of the total number of votes cast in all elections.	Try to modify protective counter.	No access could be gained to the eSlate or the JBC to try to bring the system down. Attempts to access ports on the machines were unsuccessful due to the proprietary OS. There are no menu options or supervisory functions that will modify the protective counter.
2.13	The eSlate shall not allow "Man-in-the-middle" attacks when communicating between the Election Management software and the eSlate.	Observe the hardware and communication architecture to determine if such attacks are possible.	The system does not support communication with a phone modem or network adapter. No "man in the middle" attack is possible.
2.14	The eSlate shall protect all COM ports from intrusions or vulnerabilities.	Try to gain access via an open TCP/UDP or serial or USB or other port.	The system does not support communication with a phone modem or network adapter.
2.15	The eSlate shall be resistant to introduction of Trojans, viruses, or any other form of malware.	Try to introduce any type of malicious software (malware) into the system.	Attempts to access ports on the machines were unsuccessful due to the proprietary OS. The MBB is on a linear card and could not be read by the Windows file system.
2.16	The system shall have a programmable memory device that is sealed in the unit with means of tamper detection.	Inspect the hardware design documents and physical hardware.	The MBB is located in the JBC. Locks or seals can be used to limit or detect unauthorized access to the memory card.
2.17	The system shall provide for safeguards against and evidence of tampering, theft or damage of the system and units.	Inspect the physical hardware for location of seals and locks.	There are no locks or seals available to limit or detect access to any elements of the JBC or MBB. The daisy chain connection between units is accessible to the voter and can be disrupted by disconnecting a serial port connection.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
2.18	In the event of the failure of a unit, the system shall retain a record of all votes cast prior to the failure.	Voted on unit, then removed power. The unit was left on overnight to drain the battery. The unit was started back up and checked for correct data.	When power was pulled or drained the memory was kept on the flash. No voting data was lost or corrupted.
Physical Testing			
3.01	There shall be a programmable memory device sealed in unit with means of tamper detection.	The MBB card should be stored in the JBC unit with means of tamper detection.	MBB card is stored in a tamper proof slot in the JBC. This can be either locked or sealed.
3.02	Poll opening reports should have all system audit information required.	Conduct accuracy and logic tests and verify system audit information is present.	Logic and accuracy tests along with poll opening reports produce reports with all system audit and election information.
3.03	The system shall store logic and accuracy test results in memory of the main unit processor and Election Day device.	Conduct logic and accuracy test before star of election. The results should be stored in the on-board memory within the JBC.	Logic and accuracy tests are stored in the memory of the JBC and audit logs verify these tests were conducted.
3.04	The system shall provide logic and accuracy tests in the memory of the main processor and the programmable memory device used on Election Day, including zero printouts before each election and a precinct tally printout at the close of each election.	Conduct logic and accuracy testing before election is started. Print a zero tape before an election and a result tape after an election.	Logic and accuracy tests were conducted before the election to verify counters are working properly and the programming for each voting device is correct. A zero tape printout was created and verified that no votes were cast before the start of the election. After voting was closed, a result tape was printed.
3.05	The system shall control logic and data processing methods to detect errors and provide correction method.	Create an instance where a known error will occur on the eSlate 3000. For instance, enter a voter card after it has been de-activated.	Error messages are presented to the user in a clear and concise format on the eSlate. This is standard throughout all error handling functions on the eSlate.
3.06	The eSlate shall provide a mechanism for executing test procedures which validate the correctness of election programming for each voting device and polling place and insure that the ballot display corresponds with the installed election program.	Conduct a logic and accuracy test before the start of an election.	Logic and accuracy tests were conducted in test mode and this process validates the correctness of all election functions and ensures ballot display corresponds with the installed election program.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.07	The EMS software shall not allow unauthorized modification of the Ballot Definition data.	Try to modify the vote tally in the BOSS software using a tool such as MS Excel or MS Access.	The BOSS software uses Sybase SQLAnywhere 7.0 to store results. The Database has been configured using Microsoft's ODBC drivers. The passwords have been hard coded in the driver properties. Using MS Access from the Administrator account we were able to create an external link to the BOSS, SERVO, and TALLY databases and read and manipulate the data. Hart limits the privileges of all other functional accounts which effectively prevents users from accessing the database in this manner.
3.08	The system shall present the ballot to the voter in a clear and unambiguous manner.	Create an election ballot definition file and transfer the file to the JBC. Open election on eSlate 3000 and look at ballot.	The ballot is presented to the user in a clear and unambiguous manner.
3.09	The eSlate shall not allow voters to vote multiple times.	Not applicable. There was only one test scenario for this requirement for Hart InterCivic; see 3.10 below.	Not applicable. There was only one test scenario for this requirement for Hart InterCivic; see 3.10 below.
3.10	The eSlate shall not allow voters to vote multiple times.	Enter an authorized PIN into the eSlate 3000 and try to use it to vote multiple times.	PIN numbers are unique and only used once. Once the ballot has been cast the PIN number is de-activated. An attempt to vote twice was unsuccessful.
3.11	The system shall not allow voting access to unauthorized persons.	Vote without accessing a Voter MBB.	JBC will not work without a MBB inserted. Election records cannot be stored without a MBB. An error message on the JBC is presented to the user.
3.12	The eSlate shall not allow viewing or changing vote results during the election process.	Insert a MBB in the JBC and try to view or change vote results.	JBC will not allow a user to change results and only when the election is closed can a user print results.
3.13	The eSlate shall not allow the accidental or unauthorized closing of the election.	Insert a MBB in the JBC and try to terminate the election early.	If configured in the BOSS software, a password is necessary to close election early. However, the BOSS software will allow a zero-length password.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.14	The eSlate shall not allow the accidental or unauthorized reset of the eSlate.	Insert a MBB in the JBC and try to reset the JBC.	The JBC cannot be reset using an MBB. The JBC must be connected to the computer with the Servo software. The JBC can be reset using a menu option within the Servo software.
3.15	The eSlate shall not allow the use of an unauthorized PIN to access supervisor functions.	Access the supervisor functions on the JBC.	Any user can access the supervisor functions on the JBC with a password and access to the JBC.
3.16	The eSlate shall not lose voter information, vote count, Ballot Definition information, etc. due to a power outage during the election.	Start voting on the eSlate 3000, and then disconnect batteries/power for 30 minutes to simulate a power outage to both voting terminal and the JBC, Resume power and start up the voting terminal and JBC, and check the voter information.	eSlate has no power source. The JBC controls the access to the eSlate and the JBC was unplugged and plugged back in with no lost votes.
3.17	The eSlate shall not lose voter information, vote count, Ballot Definition information, etc. due to a power outage during the election.	Start voting on the eSlate 3000, and then disconnect power for thirty minutes to simulate a power outage to both voting terminal and JBC, and then resume power. Cast votes before, during, and after the disruption.	JBC and eSlate units have no power source or battery pack. The JBC provides the power to the eSlates. The JBC was unplugged and plugged back in with no lost votes.
3.18	The eSlate shall not allow for modification of the "protective counter" which tracks the total number of votes cast on the machine.	Try to modify the protective counter on the eSlate 3000.	Supervisor function will not allow the altering of counts on the eSlate voting machine. Counter is stored within the CPU on the eSlate. The number on the counter is printed out before the election and after the election as well.
3.19	The eSlate shall not allow modification that forces it to use the same storage device for all of the data.	Try to modify the eSlate 3000 so that it unknowingly stores data and backups of data in the same location.	The MBB card must be in the slot on the JBC or the election will not open. Information is stored on this card and the flash memory within the eSlate.
3.20	The system shall not allow supervisor access to unauthorized persons.	Access the JBC supervisor functions using the password created in BOSS.	User can access supervisor functions with access to the JBC and a password.
3.21	The audit logs shall record all instances of supervisor access to the eSlate.	Review audit log after completing successful vote and verify all instances of supervisor access is logged.	Audit logs record all instances of supervisor access.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.22	The system audit log shall contain sufficient information to allow the auditing of all operations related to central site ballot tabulation, results consolidation, and report generation. It shall include a/an: • Identification of the program and version being run • Identification of the election file being used • Record of all options entered by the operator • Record of all actions performed by the subsystem • Record of all tabulation and consolidation input	Conduct an election. Print the audit log from the JBC and check for the required data.	Audit log has sufficient information to allow a complete and thorough audit of a specific eSlate within a precinct. All necessary information is included within the audit logs.
3.23	The system audit log must be created and maintained by the system in the sequence in which operations were performed.	Review audit log after completing successful vote test and ensure each step, which used supervisor access, is correctly sequenced.	The audit log is generated in sequential order and each transaction within the audit log is time stamped.
3.24	The system audit log must be created and maintained by the system in the sequence in which operations were performed.	Conduct an election. Print the audit log from the JBC and check for the data to be printed in the sequence in which operations were performed.	The audit is time stamped and sequenced to all actual events that occurred on the eSlate.
3.25	The system shall provide for safeguards against and evidence of tampering, theft or damage of the system and units.	The JBC and eSlate 3000 should contain Tamper-evident seals for the MBB card.	MBB cards can be locked or sealed in the JBC.
3.26	The media/medium in which vote counts are transferred to the Tally software shall not allow modification of the vote count.	Try to access vote records on the MBB before transferring to BOSS software.	The MBB is on a linear card and could not be read by the Windows file system. Vote counts could not be altered on the MBB card.
3.27	The system shall ensure that a voter's exact voting record cannot be traced back to the voter.	Try to access the information needed to reconstruct a voter's exact voting record.	Individual vote records are not reported from the eSlate or tally software. The voting records are not kept in any specific order and the voter is kept anonymous. The system will provide for provisional voting by creating a sequence to list provisional voter records.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.28	The system shall prevent modification of the voter's vote after the ballot is cast.	Attempt to change a vote, after it is cast, on the eSlate 3000.	A user cannot alter a vote once the ballot has been cast. There is no supervisor function to allow for the votes cast to be altered.
3.29	The system shall protect the secrecy of the vote such that the vote may not be observed during the voter's selection of preferences, during the casting of the ballot, and as the voted ballot is transmitted for recording on a storage device.	When the vote is being cast, others should not be allowed to view the voter's selection of preferences.	Curtains are provided on the voting booth to allow a voter to have secrecy during voting.
3.30	The system shall prohibit voted ballots from being accessed by anyone until after the close of polls.	Verify reports can only be executed after the polls have been closed.	Supervisor functions to print reports are not available until the polls are closed. Reports can only be created after polls have closed.
3.31	The system shall provide that each voter's ballot is secret and the voter cannot be identified by image, code or other methods.	Conduct a mock election and cast votes. Close the election and print out a record of each individual vote cast.	Individual voting records are not available for each voter. Provisional voting functionality is available as required.
3.32	The system shall provide a summary screen at the end of the ballot showing what the voter has chosen prior to the final vote being cast.	Vote for all issues and/or candidates and before casting the ballot, verify a summary of all votes is presented.	The eSlate presents the user with a summary of all votes for each race/issue. The voter can change votes at this point before the ballot is cast.
3.33	The eSlate shall not allow unauthorized modification to its operating system.	Try to modify the operating system on the eSlate 3000 by loading a program in the MBB card (The eSlate 3000 gets the ballot definition from the MBB card in the JBC).	An attempt was made to load a program on the operating system and the attempt was unsuccessful. The operating system did not recognize the program loaded.
3.34	The eSlate shall not allow printing of summary reports before the sequence of events required for closing of the polls are completed.	Try to print out any reports from the eSlate 3000 before election has been closed.	The eSlate 3000 will not allow any printed reports of votes cast or vote totals until election is closed.
3.35	There shall be no loss of data during generation of reports including results, images and inaccurate vote counts.	Print reports after close of an election and verify that the reports were printed correctly by matching it with the actual tally on the JBC.	No loss of data during the report generation.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.36	The system shall provide printed records regarding the opening and closing of the polls and include the following: • Identification of election, including opening and closing date and times • Identification of each unit • Identification of ballot format • Identification of candidate and/or issue, verifying zero start • Identification of all ballot fields and all special voting options • Summary report of votes cast for each device, or ability to extract same	Close the election and print out a copy of the audit log and review all transactions.	Audit logs are stored within the MBB for each eSlate and can viewed using the SERVO software. The software allows for the printing of these audit logs and all necessary information is included within the audit logs.
3.37	The system shall produce a paper audit trail. To guard against fraud, systems shall not produce individual paper records that voters could remove from the polling place.	Conduct an election. Cast votes. Check whether the eSlate 3000 terminal and JBC produces a paper trail for individual voters.	Audit logs are created for each eSlate to provide a specific audit trail to safeguard against fraud.
3.38	The system shall provide printout results containing candidates and/or issues in an alphanumeric format next to the vote totals.	Conduct a mock election and cast multiple votes. Once the voting is closed, print out results of the election using the supervisor functions.	Election results were printed out with Tally software and a number of different reports were created to highlight specific areas.
3.39	The system shall allow for extraction of data from memory devices to a central host.	The MBB card should contain the totals for the JBC, which can be transferred to the central host.	The MBB is used to store data in the JBC and is used to transfer results to Tally software.
3.40	The Tally software shall not allow the double counting of votes from a precinct or eSlate.	Upload election results from the eSlate 3000 to the Tally software. Upload them a second time.	Unable to upload results twice. An error message is clearly presented to the user.
3.41	The Tally software shall not allow modification of the vote count.	Try to modify the vote tally in the Tally software using a tool such as MS Excel or MS Access.	The BOSS software uses Sybase SQLAnywhere 7.0 to store results. The Database has been configured using Microsoft's ODBC drivers. The passwords have been hard coded in the driver properties. Using MS Access we were able to create an external link to the BOSS, SERVO, and Tally databases and read and manipulate the data.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.42	The system shall provide for summary reports of votes cast on each voting device by extracting information from a memory device or a removable data storage device.	Conduct an election. Cast votes. Close the election. Print summary reports from JBC using the MBB card.	Summary reports are available for each precinct. The summary report is an accurate reflection of the votes cast. The results are stored in three places: the removable MBB, internal flash memory in the eSlate, and internal flash memory in the JBC.
3.43	The system shall provide for easily downloading results from balloting into the final tally of votes.	Conduct a mock election and have multiple voters cast ballots. Once the election is closed, the transferring of votes to BOSS software for tallying and reporting is done.	Once the votes have been cast, the MBB must be inserted in the MBB reader and downloaded to the Tally Software.
3.44	The system shall accurately report all votes cast.	Set up a mock election and cast multiple votes. Verify all votes have been included in reports created by BOSS.	All votes cast have been included in counts recorded by Tally software. All reports in Tally software accurately reflect number of votes cast on eSlate.
3.45	The system shall provide a cumulative, canvass and precinct report of absentee voting, provisional ballot voting and Election Day voting as one total.	Verify election management software has the ability to handle provisional and absentee ballot voting.	Tally software provides a complete canvass of all voting types, i.e., absentee, provisional, and reports on all these different voting types.
3.46	The system shall provide a cumulative, canvass and precinct report of Election Day Voting as one total.	Complete an election. Print the reports from the Host computer.	Reports can be structured to outline all different voting types and how many votes were cast for each type.
3.47	The system shall not lose votes, corrupt media or have performance issues due to the presence of a magnetic field.	A magnet is placed on the LCD unit on the eSlate, JBC and MBB when voting.	There was no visible degradation on the display. During voting, the magnetic field did not affect the eSlate, JBC and the MBB and no votes were lost.

Step 4: Controls Analysis

The Secretary of State has not been required to have a security plan in place for electronic voting systems in the past. As a result of HAVA, the requirement now exists.

Based on the findings of this report and the report developed by InfoSENTRY, the Secretary of State will develop a new security plan or modify the existing security plan to include risk mitigation strategies to minimize or eliminate the likelihood of threat.

Step 5: Threat Likelihood

In Step 5, the assessment team examined the threats identified in Step 2 against each potential vulnerability, and assigned a likelihood rating. The likelihood rating indicates the probability that a potential vulnerability may be exercised, taking into account the nature of the threat, motivation and capability of the threat-source (if human), and existence and effectiveness of current controls.

Each potential vulnerability was assigned a threat likelihood rating of High, Medium, or Low. The following table lists the potential vulnerabilities identified and their likelihood rating.

Potential Vulnerability Identified	Threat Likelihood Rating
Hacking	Low
System intrusion, break-ins –Physical	Low
Unauthorized system access- Physical	Low
Fraudulent act	Low
Information bribery	Low
Spoofing	Low
System intrusion	Low
Bomb/Terrorism	Low
Information warfare	Low
System attack	Low
System penetration	Low
System tampering	Low
Economic exploitation	Low
Information theft	Low
Intrusion on personal privacy	Low
Unauthorized system access (access to classified, proprietary, and/or technology-related information)	Low
Unauthorized system access	Low
System sabotage	Low
System bugs	Low
Malicious code	Low
Fraud and theft	Low
Input of falsified, corrupted data	Low
Interception	Low

Step 6: Impact Analysis

In Step 6, the assessment team determined the adverse impact(s) that would likely occur if a threat-source were able to successfully exploit a vulnerability or weakness. The team followed the process below to determine the adverse impact resulting from a successful exploitation of a vulnerability:

- Determined the criticality of the electronic voting system and data to accomplishing the SOS' mission.
- Determined the probable adverse impact of a successful exploitation of a vulnerability.
- Determined the adverse impact of a security event in regard to loss or degradation of the system's integrity, availability, and confidentiality.
- Assigned a rating of High, Medium, or Low to each vulnerability to indicate the magnitude of impact resulting from a successful exploitation of the vulnerability.

The following table shows the magnitude of impact rating that was assigned to each potential vulnerability.

Potential Vulnerability Identified	Magnitude of Impact Rating
Code Review	
Third Party Software: The eSlate and JBC units use the Mqx 2.4 Operating system and the source code for the operatng system is owned by Hart. The procedures for updating the firmware are not provided.	Medium
Database security: BOSS and Tally software (EMS) have security implemented by providing various access levels to users. User passwords are not encrypted but stored as plain text. Also database access id's and passwords are compiled into the PowerBuilder application executable and is viewable using the TextPad editor.	High
Data Model: The Data model provided in the soft and hard copy documentation is not clear. The data dictionary did not indicate the presence of primary keys.	Low
Encryption: No published encryption methodology is used in the system to protect the ballot information, cast vote records, audit logs, passwords and during data transmission between eSlate and JBC units.	Low
Platform Review	
Locks are not in place to secure the MBB card on the JBC.	High
The password is default from Hart for the eSlate unit.	Medium

Continued on the next page

Step 6: Impact Analysis (continued)

Potential Vulnerability Identified	Magnitude of Impact Rating
Physical Testing	
The JBC is a stand-alone unit that each eSlate is connected with. If a vote official is not constantly sitting with the JBC, then any individual with the correct password can close an election and print results before the election is officially closed.	Low
A MBB in transit to election central could be corrupted. A user may decide to put a corrupt program or file on the MBB to corrupt the card so votes cannot be read.	Medium
The JBC can have 12 eSlate voting machines attached for election control. Since the eSlate voting machines are daisy chained, if the first eSlate voting machine in the sequence is unplugged, the votes for the remaining 11 eSlate voting machines will not transfer to the JBC as well.	Low

Step 7: Determine Risks

The purpose of Step 7 is to assess the level of risk to the electronic voting system. In this step, the assessment team identified the risk(s), if any, arising out of each test scenario. After identifying the risks, the team assigned a risk rating for each vulnerability by combining the results of the Impact Analysis established in Step 6 with the Likelihood of Threat established in Step 5. The combination of the impact analysis and the threat likelihood versus the security controls in place were applied to a risk-level matrix to determine the resultant risk-level.

Risks Identified

The assessment team identified the following vulnerabilities of the eSlate 3000 voting system. For each vulnerability identified, the table lists the relevant requirement tested, test scenario, and test results which identified the vulnerability.

No.	Test Scenario	Test Result	Risk Identified
Code Review			
1.01	Perform visual review of source files. Function names will be checked for proper case formatting of concatenated words. Names of functions should clearly describe its purpose.	The function names are in proper and consistent case format and the names describe the high level purpose of the function.	None.
1.02	Perform visual review of source files. Modules should contain a consistent format and location for module components. Modules should begin with comments describing the modules contents. Location of methods and variables with associated comments should be consistent throughout.	Modules are consistent with respect to the format of comments and location of methods and variables.	None.
1.03	Perform visual review of source code. Modules should use a clear methodology of construction. Files will be reviewed to see if a coding industry standard is used in the naming of modules, functions, variables and constants.	Module construction appears to be consistent throughout the source code. The code uses a consistent naming standard.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.04	Perform visual review of source code. Function and variable names should be "self documenting" as well as contain properly typed and sized attributes, and return types.	The function and variable names describe their purpose. Proper attribute and return types are used in the code. Library descriptions are very informative.	None.
1.05	Perform visual review of source code for implementation of error handling code. All methods should contain error-handling logic. Systems should remain stable in the event of an error. When an error occurs, sufficient information regarding the state of the system and system parameters should be recorded for future debugging.	Review of the code indicates that error-handling code has been implemented. Error-handling code returns clear messages to the users in the event of errors. There are safeguards to prevent the system from crashing. The error and audit log entries are tracked in the eSlate.	None.
1.06	Perform visual review of source code. Comments will be reviewed for simple descriptive content. Comments should appear at the beginning of each module, function. All module level variables, constants, and structures should be commented as well. Function parameters and return values should describe appropriate values. Comments should also appear in methods to help clarify complex code and logic behind expressions.	Comments are present at the beginning of modules and briefly describe their purpose. Functions and methods contain comments describing their purpose. Module level variables, constants and structures are commented, and those that are not commented have self-describing names to identify their purpose.	None.
1.07	Perform visual review of source code. Comments should have a common format with standard fields for information. Some standard fields should be a description, parameters, return types, a change log.	The comments are in a common format containing entries including change log and describing function and module purpose.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.08	Perform visual review of source code. Modules should have a standard comment identifier at the beginning of each module. Module comments should contain the name and description of the module, a copyright notice, and a change log.	Module comments contain name, description, and a detailed change log. Copyright information is also available at the beginning of modules.	None.
1.09	Perform visual review of the source code. Modules will be reviewed for their functional content. The variables and functions should be closely related and work directly to perform a clear task.	Modules perform clearly specified tasks. Unused variables and functions were not found in the code.	None.
1.10	The source code will be visually reviewed to verify if the code has been properly modularized. Modules should be an appropriate length and encapsulate related functionality.	Several modules have been created based on functionality and code is reused in the system. The modules are of reasonable length.	None.
1.11	The source code will be visually reviewed for the use of simple and clear logical structures. There should be the use of constants and structures to improve code readability and reliability.	Constants (consts) and data structures (structs) are used wherever necessary in the code to improve readability and reliability.	None.
1.12	The source code will be visually reviewed to verify if the code has been properly modularized. Modules should encapsulate related functionality into logical groupings with clear interfaces. Interfaces should be well defined as to their use.	The code is properly modularized and the module size is managed correctly by implementing necessary functionality.	None.
1.13	The source code will be visually reviewed to verify implementation of classes and proper modularization of the source files.	Most of the MBB creation utility and PVS code is written in C. C does not implement classes, so they have not been used. But proper modularization of code is done.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.14	The source code will be visually reviewed. The name and description of the class should be simple and clear. The task performed by the function should be easy to understand, simple to define, and atomic.	The code has many modules and each implements specific functionality. The module size is appropriate and the code is readable and easy to understand.	None.
1.15	The source code will be visually reviewed to find any use of third party products. The makers and the versions of any found third party applications will be noted.	The eSlate and JBC uses an Mqx 2.4 Operating System. The source code for this operating system is currently owned and maintained by Hart InterCivic.	None.
1.16	If the source is available for any used third party products, the source will be reviewed for client modifications. Third party source code should only contain the necessary functionality with unused areas removed or disabled. If the source is not available then further study will be required.	The source code only contains the necessary functionality for the JBC and eSlate units. Other in-house developed utilities are also packaged with the Mqx operating system.	None.
1.17	The data model and database source code will be reviewed for existence of proper keys and normalization.	The eSlate does not use a database. Data files are stored in internal and external memory (MBB) in binary format. The Boss and Tally applications use a common SQLAnywhere database. The data dictionary did not indicate primary keys.	None.
1.18	The source code will be visually reviewed for user access levels and roles implemented as part of security.	Not applicable to the design of Hart InterCivic eSlate.	None.
1.19	Source code will be reviewed and tested in order to check for CRC techniques in verifying the correctness of data that is stored in memory. Can the software identify data that has been improperly modified?	CRC 16 algorithm has been implemented in the code. CRC checks are performed every time data is written to the MBB or internal memory of eSlate machines and Judge's Booth Controller. The checks are also done when data is transmitted from each eSlate to the JBC unit.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.20	The source code will be reviewed to make sure that an algorithm is implemented to make sure voter records are stored in random order. The Cast Vote Records should not have time stamp associated with it.	The vote records are stored randomly in the storage media (MBB, internal memory of eSlate and JBC). An appropriate algorithm is implemented in the code to store the data randomly and without time stamp.	None.
1.21	The source code will be reviewed to verify the system is secure and allows each voter to only vote once by issuing unique access codes.	The source code for JBC generates unique access codes for a precinct. Voters use these codes to access the eSlate device and cast their votes. These access codes are valid only for a specified time (which is set in the BOSS system) and eSlate device does not accept these codes after that time has expired.	None.
1.22	The source code will be reviewed to verify there is a means by which votes can be recovered incase of a system disaster.	Vote and audit information is stored in 3 places – MBB, internal memory in eSlate, and JBC. In the event of a disaster, the SERVO software can re-create MBBs with data from either the JBC or eSlate devices. System alerts are given in case of errors during data transmission between eSlate units and JBC.	None.
1.23	The strength of encryption will be reviewed. The types of encryption will be reviewed to see if it is sufficient.	No published encryption methodology is used in the system.	Hart does not use encryption to protect data on the eSlate 3000 and JBC. There is a risk that an unauthorized person could gain access to the data on the eSlate 3000.
1.24	Ballot Definitions and Cast Vote Records should be protected and be verifiable they are correct. Encryption should be powerful enough to block access to stored data.	Code is not available to encrypt ballot definition and cast vote records in the eSlate. But the data is stored in proprietary binary format.	Hart does not use encryption to protect data on the eSlate 3000 and JBC. There is a risk that an unauthorized person could access ballot definitions and cast vote records on the JBC.
1.25	Various means of "voter identification" should be secure. The data on a voter authorization token should not be discernable.	The voter is identified to the eSlate based on a four-digit PIN generated by the JBC. Based on code review, the voter information is not stored anywhere in the system.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.26	Encryption keys should be randomly generated every time and sufficiently long so that it is not easy to guess. The key itself should be kept private and not easily discovered.	No published encryption methodology is used in the system.	None.
1.27	Transmission protocols will be checked for the use on encryption. Data should never travel over a wire without protection. The contents of the transmission should be verifiable as to their contents and correctness. Any type of tampering should be identifiable if not impossible.	Communication between JBC and eSlate units uses RS485 protocol. The data transmitted between these units is not encrypted. After the polls are closed, the MBBs or eSlate units are physically transported to the computer(s) at a central location and are read by the Tally or SERVO software to tally the results.	Hart does not use encryption to protect data on the eSlate 3000 and JBC. There is a risk that an unauthorized person could intercept and view election data.
1.28	Check the vote records on the Mobile Ballot Box, Ballot Origination Software, Tally and Servo software, and transfer medium to ensure that the records are encrypted.	No published encryption methodology is used in the system.	Same as 1.24 – Hart does not use encryption to protect data on the eSlate 3000 and JBC. There is a risk that an unauthorized person could access ballot definitions and cast vote records on the JBC.
1.29	Check the audit logs on the PVS to ensure that they are encrypted.	No published encryption methodology was found to store audit log information.	Hart does not use encryption to protect data on the eSlate 3000 and JBC. There is a risk that an unauthorized person could access audit log information.
1.30	Perform code review to ensure that passwords used in all software are encrypted.	No published encryption methodology is used in the system to protect the passwords.	The Hart eSlate 3000 and JBC does not use a supervisory mode but do optionally provide passwords. There is a risk that an unauthorized person could gain access to Supervisor functions in the JBC.
1.31	Perform code review to ensure that the system does not use hardcoded passwords.	Hardcoded passwords are not used in the system.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
Platform Review			
2.01	Attempt to gain access to the system in supervisor mode.	There is not a supervisor mode on the Hart eSlate.	None.
2.02	Try to modify the Ballot Definition file on the MBB card before loading it on the eSlate.	The MBB is on a linear card and could not be read by the Windows file system. We were unable to modify the ballot definition file while it was on the MBB.	None.
2.03	Install a program on a MBB card, insert it in the eSlate, and install and/or execute the unauthorized program.	The MBB is on a linear card and could not be read by the Windows file system. We were unable to place a counterfeit program on the MBB.	None.
2.04	Inspect the eSlate for network accessible ports.	The eSlate has two serial ports used to connect to the eSlate on either side of the daisy chain. The JBC has three serial ports. One is used for a 9600 baud modem connection. One goes to the first eSlate, and one goes to a printer. The ports that are on the eSlate could not be used for network communication.	None.
2.05	Try to access, modify, or disrupt the functioning of the JBC or eSlate software while connected to a network.	The JBC cannot be connected to a network. A modem port is present but has been disabled in this version.	None.
2.06	Try to bring the system down, lock up the operating system, change or erase log files, or any other form of Denial of Service (DoS), Distributed Denial of Service (DDos), or other result which benefits the attacker.	Attempts to disrupt the JBC using the ports on the machine were unsuccessful due to limitations of the proprietary OS.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
2.07	Try to gain supervisor rights or system rights by any means necessary.	There are no supervisor modes on the JBC or eSlate. Access to supervisor function is limited by physical access to the JBC.	Access to supervisor functions, which are limited to opening and closing the polls, is controlled by physical access to the JBC and an optional password set in the BOSS election management software. There is a risk that an unauthorized person could perform supervisory functions by gaining physical access to the JBC.
2.08	Try to cause a kernel panic, system failure, or indefinite wait state, or other operating system lock-up within the operating system or sub-system.	The MBB is on a linear card and could not be read by the Windows file system. No access could be gained to the eSlate or the JBC to try to bring the system down. Attempts to access ports on the machines were unsuccessful due to the proprietary OS.	None.
2.09	Observe that functions are password protected, the minimum length of passwords, and that they can be changed.	The password can be changed within the BOSS software. The minimum length of the password is zero.	Access to supervisor functions, which are limited to opening and closing the polls, is controlled by physical access to the JBC and an optional password set in the BOSS election management software. There is a risk that an unauthorized person could perform supervisory functions by gaining physical access to the JBC.
2.10	Try to create an attack on flash memory using files loaded on the MBB card.	The MBB is on a linear card and could not be read by the Windows file system.	None.
2.11	Change the contents on a removable media card and use the card. Determine if the system reports the card has been modified.	The MBB is on a linear card and could not be read by the Windows file system.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
2.12	Try to modify protective counter.	No access could be gained to the eSlate or the JBC to try to bring the system down. Attempts to access ports on the machines were unsuccessful due to the proprietary OS. There are no menu options or supervisory functions that will modify the protective counter.	None.
2.13	Observe the hardware and communication architecture to determine if such attacks are possible.	The system does not support communication with a phone modem or network adapter. No "man in the middle" attack is possible.	None.
2.14	Try to gain access via an open TCP/UDP or serial or USB or other port.	The system does not support communication with a phone modem or network adapter.	None.
2.15	Try to introduce any type of malicious software (malware) into the system.	Attempts to access ports on the machines were unsuccessful due to the proprietary OS. The MBB is on a linear card and could not be read by the Windows file system.	None.
2.16	Inspect the hardware design documents and physical hardware.	The MBB is located in the JBC. Locks or seals can be used to limit or detect unauthorized access to the memory card.	None.
2.17	Inspect the physical hardware for location of seals and locks.	There are no locks or seals available to limit or detect access to any elements of the JBC or MBB. The daisy chain connection between units is accessible to the voter and can be disrupted by disconnecting a serial port connection.	The JBC is connected to each eSlate 3000 using a daisy-chained cable. The daisy chain connection between units is accessible to the voter and can be disrupted by disconnecting a serial port connection. Once disconnected, the JBC must be power cycled to bring the disconnected eSlates back on line. There is a risk that an unauthorized person can disconnect the daisy chain connection between the JBC and eSlate 3000, causing a disruption in voting.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
2.18	Voted on unit, then removed power. The unit was left on overnight to drain the battery. The unit was started back up and checked for correct data.	When power was pulled or drained the memory was kept on the flash. No voting data was lost or corrupted.	None.
Physical Testing			
3.01	The MBB card should be stored in the JBC unit with means of tamper detection.	MBB card is stored in a tamper proof slot in the JBC. This can be either locked or sealed.	None.
3.02	Conduct accuracy and logic tests and verify system audit information is present.	Logic and accuracy tests along with poll opening reports produce reports with all system audit and election information.	None.
3.03	Conduct logic and accuracy test before star of election. The results should be stored in the on-board memory within the JBC.	Logic and accuracy tests are stored in the memory of the JBC and audit logs verify these tests were conducted.	None.
3.04	Conduct logic and accuracy testing before election is started. Print a zero tape before an election and a result tape after an election.	Logic and accuracy tests were conducted before the election to verify counters are working properly and the programming for each voting device is correct. A zero tape printout was created and verified that no votes were cast before the start of the election. After voting was closed, a result tape was printed.	None.
3.05	Create an instance where a known error will occur on the eSlate 3000. For instance, enter a voter card after it has been de-activated.	Error messages are presented to the user in a clear and concise format on the eSlate. This is standard throughout all error handling functions on the eSlate.	None.
3.06	Conduct a logic and accuracy test before the start of an election.	Logic and accuracy tests were conducted in test mode and this process validates the correctness of all election functions and ensures ballot display corresponds with the installed election program.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.07	Try to modify the Ballot Definition in the BOSS software using a viewer/program.	The BOSS software uses Sybase SQLAnywhere 7.0 to store results. The Database has been configured using Microsoft's ODBC drivers. The passwords have been hard coded in the driver properties. Using MS Access from the Administrator account we were able to create an external link to the BOSS, SERVO, and TALLY databases and read and manipulate the data. Hart limits the privileges of all other functional accounts which effectively prevents users from accessing the database in this manner.	There is a risk that an unauthorized person with access to the administrator account on the system might use or install any basic data access program that uses ODBC for it's bridge to read and modify the data contained in the Ballot and Tally databases.
3.08	Create an election ballot definition file and transfer the file to the JBC. Open election on eSlate 3000 and look at ballot.	The ballot is presented to the user in a clear and unambiguous manner.	None.
3.09	Not applicable. There was only one test scenario for this requirement for Hart InterCivic; see 3.10 below.	Not applicable. There was only one test scenario for this requirement for Hart InterCivic; see 3.10 below.	Not applicable. There was only one test scenario for this requirement for Hart InterCivic; see 3.10 below.
3.10	Enter an authorized PIN into the eSlate 3000 and try to use it to vote multiple times.	PIN numbers are unique and only used once. Once the ballot has been cast the PIN number is de-activated. An attempt to vote twice was unsuccessful.	None.
3.11	Vote without accessing a Voter MBB.	JBC will not work without a MBB inserted. Election records cannot be stored without a MBB. An error message on the JBC is presented to the user.	None.
3.12	Insert a MBB in the JBC and try to view or change vote results.	JBC will not allow a user to change results and only when the election is closed can a user print results.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.13	Insert a MBB in the JBC and try to terminate the election early.	If configured in the BOSS software, a password is necessary to close election early. However, the BOSS software will allow a zero-length password.	Access to supervisor functions, which are limited to opening and closing the polls, is controlled by physical access to the JBC and an optional password set in the BOSS election management software. No warning is provided if the user tries to close the polls before the scheduled end of the election. If the polls are closed prematurely, all eSlates attached to the JBC will be closed. There is a risk that an unauthorized person could access the JBC and close the polls prematurely.
3.14	Insert a MBB in the JBC and try to reset the JBC.	The JBC cannot be reset using an MBB. The JBC must be connected to the computer with the Servo software. The JBC can be reset using a menu option within the Servo software.	None.
3.15	Access the supervisor functions on the JBC.	Any user can access the supervisor functions on the JBC with a password and access to the JBC.	Access to supervisor functions, which are limited to opening and closing the polls, is controlled by physical access to the JBC and an optional password set in the BOSS election management software. There is a risk that an unauthorized person could access supervisor functions.
3.16	Start voting on the eSlate 3000, and then disconnect batteries/power for 30 minutes to simulate a power outage to both voting terminal and the JBC, Resume power and start up the voting terminal and JBC, and check the voter information.	eSlate has no power source. The JBC controls the access to the eSlate and the JBC was unplugged and plugged back in with no lost votes.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.17	Start voting on the eSlate 3000, and then disconnect power for thirty minutes to simulate a power outage to both voting terminal and JBC, and then resume power. Cast votes before, during, and after the disruption.	JBC and eSlate units have no power source or battery pack. The JBC provides the power to the eSlates. The JBC was unplugged and plugged back in with no lost votes.	None.
3.18	Try to modify the protective counter on the eSlate 3000.	Supervisor function will not allow the altering of counts on the eSlate voting machine. Counter is stored within the CPU on the eSlate. The number on the counter is printed out before the election and after the election as well.	None.
3.19	Try to modify the eSlate 3000 so that it unknowingly stores data and backups of data in the same location.	The MBB card must be in the slot on the JBC or the election will not open. Information is stored on this card and the flash memory within the eSlate.	None.
3.20	Access the JBC supervisor functions using the password created in BOSS.	User can access supervisor functions with access to the JBC and a password.	Same as 3.15 – Access to supervisor functions, which are limited to opening and closing the polls, is controlled by physical access to the JBC and an optional password set in the BOSS election management software. There is a risk that an unauthorized person could access supervisor functions.
3.21	Review audit log after completing successful vote and verify all instances of supervisor access is logged.	Audit logs record all instances of supervisor access.	None.
3.22	Conduct an election. Print the audit log from the JBC and check for the required data.	Audit log has sufficient information to allow a complete and thorough audit of a specific eSlate within a precinct. All necessary information is included within the audit logs.	None.
3.23	Review audit log after completing successful vote test and ensure each step, which used supervisor access, is correctly sequenced.	The audit log is generated in sequential order and each transaction within the audit log is time stamped.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.24	Conduct an election. Print the audit log from the JBC and check for the data to be printed in the sequence in which operations were performed.	The audit is time stamped and sequenced to all actual events that occurred on the eSlate.	None.
3.25	The JBC and eSlate 3000 should contain Tamper-evident seals for the MBB card.	MBB cards can be locked or sealed in the JBC.	None.
3.26	Try to access vote records on the MBB before transferring to BOSS software.	The MBB is on a linear card and could not be read by the Windows file system. Vote counts could not be altered on the MBB card.	None.
3.27	Try to access the information needed to reconstruct a voter's exact voting record.	Individual vote records are not reported from the eSlate or tally software. The voting records are not kept in any specific order and the voter is kept anonymous. The system will provide for provisional voting by creating a sequence to list provisional voter records.	None.
3.28	Attempt to change a vote, after it is cast, on the eSlate 3000.	A user cannot alter a vote once the ballot has been cast. There is no supervisor function to allow for the votes cast to be altered.	None.
3.29	When the vote is being cast, others should not be allowed to view the voter's selection of preferences.	Curtains are provided on the voting booth to allow a voter to have secrecy during voting.	None.
3.30	Verify reports can only be executed after the polls have been closed.	Supervisor functions to print reports are not available until the polls are closed. Reports can only be created after polls have closed.	None.
3.31	Conduct a mock election and cast votes. Close the election and print out a record of each individual vote cast.	Individual voting records are not available for each voter. Provisional voting functionality is available as required.	None.
3.32	Vote for all issues and/or candidates and before casting the ballot, verify a summary of all votes is presented.	The eSlate presents the user with a summary of all votes for each race/issue. The voter can change votes at this point before the ballot is cast.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.33	Try to modify the operating system on the eSlate 3000 by loading a program in the MBB card (The eSlate 3000 gets the ballot definition from the MBB card in the JBC).	An attempt was made to load a program on the operating system and the attempt was unsuccessful. The operating system did not recognize the program loaded.	None.
3.34	Try to print out any reports from the eSlate 3000 before election has been closed	The eSlate 3000 will not allow any printed reports of votes cast or vote totals until election is closed.	None.
3.35	Print reports after close of an election and verify that the reports were printed correctly by matching it with the actual tally on the JBC.	No loss of data during the report generation.	None.
3.36	Close the election and print out a copy of the audit log and review all transactions.	Audit logs are stored within the MBB for each eSlate and can viewed using the SERVO software. The software allows for the printing of these audit logs and all necessary information is included within the audit logs.	None.
3.37	Conduct an election. Cast votes. Check whether the eSlate 3000 terminal and JBC produces a paper trail for individual voters.	Audit logs are created for each eSlate to provide a specific audit trail to safeguard against fraud.	None.
3.38	Conduct a mock election and cast multiple votes. Once the voting is closed, print out results of the election using the supervisor functions.	Election results were printed out with Tally software and a number of different reports were created to highlight specific areas.	None.
3.39	The MBB card should contain the totals for the JBC, which can be transferred to the central host.	The MBB is used to store data in the JBC and is used to transfer results to Tally software.	None.
3.40	Upload election results from the eSlate 3000 to the Tally software. Upload them a second time.	Unable to upload results twice. An error message is clearly presented to the user.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.41	Try to modify the vote tally in the Tally software using a tool such as MS Excel or MS Access.	The BOSS software uses Sybase SQLAnywhere 7.0 to store results. The Database has been configured using Microsoft's ODBC drivers. The passwords have been hard coded in the driver properties. Using MS Access we were able to create an external link to the BOSS, SERVO, and Tally databases and read and manipulate the data.	An external link was created to the BOSS, Servo, and Tally databases, and the data was read and manipulated. There is a risk that the data contained in the Ballot and Tally databases can be read and modified by an unauthorized person who has access to the system and the ability to use or install any basic data access program that uses ODBC for its driver.
3.42	Conduct an election. Cast votes. Close the election. Print summary reports from JBC using the MBB card.	Summary reports are available for each precinct. The summary report is an accurate reflection of the votes cast. The results are stored in three places: the removable MBB, internal flash memory in the eSlate, and internal flash memory in the JBC.	None.
3.43	Conduct a mock election and have multiple voters cast ballots. Once the election is closed, the transferring of votes to BOSS software for tallying and reporting is done.	Once the votes have been cast, the MBB must be inserted in the MBB reader and downloaded to the Tally Software.	None.
3.44	Set up a mock election and cast multiple votes. Verify all votes have been included in reports created by BOSS.	All votes cast have been included in counts recorded by Tally software. All reports in Tally software accurately reflect number of votes cast on eSlate.	None.
3.45	Verify election management software has the ability to handle provisional and absentee ballot voting.	Tally software provides a complete canvass of all voting types, i.e., absentee, provisional, and reports on all these different voting types.	None.
3.46	Complete an election. Print the reports from the Host computer.	Reports can be structured to outline all different voting types and how many votes were cast for each type.	None.
3.47	A magnet is placed on the LCD unit on the eSlate, JBC and MBB when voting.	There was no visible degradation on the display. During voting, the magnetic field did not affect the eSlate, JBC and the MBB and no votes were lost.	None.

Risk Levels of Identified Risks

Each Threat-Source/Vulnerability was assigned a rating of High, Medium, or Low to represent the degree or level of risk to which the electronic voting system might be exposed if a given vulnerability were exercised. Following is a description of the High, Medium, and Low ratings.

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, it must determined whether corrective actions are still required or whether the risk can be accepted.

The following table shows the rating assigned to each identified risk.

No.	Risk Identified	Risk Likelihood	Impact Rating	Risk Level
Code Review				
1.23	Hart does not use encryption to protect data on the eSlate 3000 and JBC. There is a risk that an unauthorized person could gain access to the data on the eSlate 3000.	Low	Low	Low
1.24 1.28	Hart does not use encryption to protect data on the eSlate 3000 and JBC. There is a risk that an unauthorized person could access ballot definitions and cast vote records on the JBC.	Low	Medium	Low
1.27	Hart does not use encryption to protect data on the eSlate 3000 and JBC. There is a risk that an unauthorized person could intercept and view election data.	Low	Medium	Low
1.29	Hart does not use encryption to protect data on the eSlate 3000 and JBC. There is a risk that an unauthorized person could access audit log information.	Low	Low	Low
1.30	The Hart eSlate 3000 and JBC does not use a supervisory mode but do optionally provide passwords. There is a risk that an unauthorized person could gain access to Supervisor functions in the JBC.	Medium	High	Medium

Continued on the next page

Risk Levels of Identified Risks (continued)

No.	Risk Identified	Risk Likelihood	Impact Rating	Risk Level
Platform Review				
2.07	Access to supervisor functions, which are limited to opening and closing the polls, is controlled by physical access to the JBC and an optional password set in the BOSS election management software. There is a risk that an unauthorized person could perform supervisory functions by gaining physical access to the JBC.	High	High	High
2.09	Access to supervisor functions, which are limited to opening and closing the polls, is controlled by physical access to the JBC and an optional password set in the BOSS election management software. There is a risk that an unauthorized person could perform supervisory functions by gaining physical access to the JBC.	High	High	High
2.17	The JBC is connected to each eSlate 3000 using a daisy-chained cable. The daisy chain connection between units is accessible to the voter and can be disrupted by disconnecting a serial port connection. Once disconnected, the JBC must be power cycled to bring the disconnected eSlates back on line. There is a risk that an unauthorized person can disconnect the daisy chain connection between the JBC and eSlate 3000, causing a disruption in voting.	High	High	High
Physical Testing				
3.07	There is a risk that an unauthorized person with access to the administrator account on the system might use or install any basic data access program that uses ODBC for it's bridge to read and modify the data contained in the Ballot and Tally databases.	Low	High	Low
3.13	Access to supervisor functions, which are limited to opening and closing the polls, is controlled by physical access to the JBC and an optional password set in the BOSS election management software. No warning is provided if the user tries to close the polls before the scheduled end of the election. If the polls are closed prematurely, all eSlates attached to the JBC will be closed. There is a risk that an unauthorized person could access the JBC and close the polls prematurely.	High	High	High
3.15 3.20	Access to supervisor functions, which are limited to opening and closing the polls, is controlled by physical access to the JBC and an optional password set in the BOSS election management software. There is a risk that an unauthorized person could access supervisor functions.	High	High	High

Continued on the next page

Risk Levels of Identified Risks (continued)

No.	Risk Identified	Risk Likelihood	Impact Rating	Risk Level
3.41	There is a risk that an unauthorized person with access to the administrator account on the system might use or install any basic data access program that uses ODBC for it's bridge to read and modify the data contained in the Ballot and Tally databases.	Low	High	Low

Step 8: Risk Mitigation Strategies

In Step 8, the assessment team recommended solutions that are intended to mitigate or eliminate the risks identified in Step 7. The goal of the recommended risk mitigation strategies is to reduce the level of risk to the electronic voting system and its data to an acceptable level.

Recommended Risk Mitigation Strategies

The assessment team recommends the following mitigation strategies for the risks identified during this assessment.

Code Review

No.	Risk Identified	Recommended Mitigation Strategy
High Risk		
	N/A	
Medium Risk		
1.30	The Hart eSlate 3000 and JBC does not use a supervisory mode but do optionally provide passwords. There is a risk that an unauthorized person could gain access to Supervisor functions in the JBC.	We recommend the Secretary of State require that Hart InterCivic incorporate mandatory user passwords of at least six characters in length for using the JBC. We also recommend the Secretary of State require that administrative policies and procedures be put into place regarding password management.
Low Risk		
1.23	Hart does not use encryption to protect data on the eSlate 3000 and JBC. There is a risk that an unauthorized person could gain access to the data on the eSlate 3000.	We recommend the Secretary of State require that Hart InterCivic incorporate strong encryption to protect data.

Continued on the next page

Recommended Risk Mitigation Strategies (continued)

Code Review (continued)

No.	Risk Identified	Recommended Mitigation Strategy
Low Risk (continued)		
1.24 1.28	Hart does not use encryption to protect data on the eSlate 3000 and JBC. There is a risk that an unauthorized person could access ballot definitions and cast vote records on the JBC.	We recommend the Secretary of State require that Hart InterCivic incorporate strong encryption to protect data.
1.27	Hart does not use encryption to protect data on the eSlate 3000 and JBC. There is a risk that an unauthorized person could intercept and view election data.	We recommend the Secretary of State require that Hart InterCivic incorporate strong encryption to protect data.
1.29	Hart does not use encryption to protect data on the eSlate 3000 and JBC. There is a risk that an unauthorized person could access audit log information.	We recommend the Secretary of State require that Hart InterCivic incorporate strong encryption to protect data.

Platform Review

No.	Risk Identified	Recommended Mitigation Strategy
High Risk		
2.07 2.09	Access to supervisor functions, which are limited to opening and closing the polls, is controlled by physical access to the JBC and an optional password set in the BOSS election management software. There is a risk that an unauthorized person could perform supervisory functions by gaining physical access to the JBC.	We recommend the Secretary of State require that administrative policies and procedures be put into place regarding password management and physical access to the JBC. We also recommend the Secretary of State require that Hart InterCivic incorporate mandatory user passwords of at least six characters in length for using the JBC.

Continued on the next page

Recommended Risk Mitigation Strategies (continued)

Platform Review (continued)

No.	Risk Identified	Recommended Mitigation Strategy
High Risk (continued)		
2.17	The JBC is connected to each eSlate 3000 using a daisy-chained cable. The daisy chain connection between units is accessible to the voter and can be disrupted by disconnecting a serial port connection. Once disconnected, the JBC must be power cycled to bring the disconnected eSlates back on line. There is a risk that an unauthorized person can disconnect the daisy chain connection between the JBC and eSlate 3000, causing a disruption in voting.	We recommend the Secretary of State require that Hart InterCivic put into place sufficient security to prevent disconnection of the daisy chain. We also recommend the Secretary of State require that administrative policies and procedures be put into place regarding physical access to the JBC and daisy chain cables.
Medium Risk		
	N/A	
Low Risk		
	N/A	

Physical Testing

No.	Risk Identified	Recommended Mitigation Strategy
High Risk		
3.13	Access to supervisor functions, which are limited to opening and closing the polls, is controlled by physical access to the JBC and an optional password set in the BOSS election management software. No warning is provided if the user tries to close the polls before the scheduled end of the election. If the polls are closed prematurely, all eSlates attached to the JBC will be closed. There is a risk that an unauthorized person could access the JBC and close the polls prematurely.	We recommend the Secretary of State require that administrative policies and procedures be put into place regarding password management and physical access to the JBC. We also recommend the Secretary of State require that Hart InterCivic incorporate mandatory user passwords of at least six characters in length for closing the polls using the JBC. We also recommend the Secretary of State require that Hart InterCivic incorporate a warning prior to closing the polls before the scheduled end of the election.

Continued on the next page

Recommended Risk Mitigation Strategies (continued)

Physical Testing

No.	Risk Identified	Recommended Mitigation Strategy
High Risk (continued)		
3.15 3.20	Access to supervisor functions, which are limited to opening and closing the polls, is controlled by physical access to the JBC and an optional password set in the BOSS election management software. There is a risk that an unauthorized person could access supervisor functions.	We recommend the Secretary of State require that administrative policies and procedures be put into place regarding password management and physical access to the JBC. We also recommend the Secretary of State require that Hart InterCivic incorporate mandatory user passwords of at least six characters in length for closing the polls using the JBC.
Medium Risk		
	N/A	
Low Risk		
3.07 3.41	There is a risk that an unauthorized person with access to the administrator account on the system might use or install any basic data access program that uses ODBC for its bridge to read and modify the data contained in the Ballot and Tally databases.	We recommend the Secretary of State require that administrative policies and procedures be put into place to require use of proper Windows login security on the EMS server and to prevent unauthorized access, and not contain any additional software that would allow access to the EMS database.

Step 9: Document Results

In Step 9, the assessment team combined the results of Steps 1 through 8 to develop this report detailing the technical security assessment and its findings.

Conclusion

Compuware has conducted a study of the Hart eSlate 3000 voting system to identify specific security vulnerabilities that might be exploited during an election and to recommend actions to mitigate these vulnerabilities. The scope of this study has been limited to reviewing the technical implementation of the eSlate 3000 and reviewing each data stream into and from the eSlate 3000. It has not included a review of the policies, procedures, or work practices of either Hart or the Ohio Secretary of State.

Continued on the next page

Conclusion (continued)

During the course of our study, Compuware has identified several significant security issues, which left unmitigated would provide an opportunity for an attacker to disrupt the election process or throw the election results into question. These are documented above. Following careful consideration of each of these security issues, we have developed mitigation recommendations for the Secretary of State to implement which we believe will limit the likelihood of a successful attack on the election process. Provided each of these mitigation recommendations can be enacted, Compuware has concluded the Hart eSlate 3000 can be securely deployed by the Secretary of State.

Although all risks documented above must be dealt with appropriately, the most significant risk areas, which will require the most effort to mitigate, include:

Risk Identified	Recommended Mitigation Strategy
Hart does not use encryption to protect election data transferred to and from the eSlate 3000 and JBC. There is a risk that an unauthorized person could gain access to the data.	We recommend the Secretary of State require that Hart InterCivic incorporate strong encryption to protect data.
All supervisory functions are executed on the JBC which is not accessed by the voters. Supervisory functions are not password protected. There is a risk that an unauthorized person might gain access to Supervisor functions in the JBC.	We recommend the Secretary of State require that Hart InterCivic incorporate mandatory user passwords of at least six characters in length for using the JBC. We also recommend the Secretary of State require that administrative policies and procedures be put into place regarding password management and physical access to the JBC.
Each eSlate DRE is connected through a daisy chain to the next eSlate. The first eSlate is connected to the JBC. These connections are made with a screwed in serial port at the top of the eSlate easily accessed by any voter. To reconnect an eSlate if the daisy chain is disrupted in the middle requires power cycling the JBC. There is a risk that an unauthorized person might accidentally or intentionally disconnect the daisy chain connection between the JBC and eSlate, causing a disruption in voting.	We recommend the Secretary of State require that Hart InterCivic put into place sufficient security to prevent disconnection of the daisy chain. We also recommend the Secretary of State require that administrative policies and procedures be put into place regarding physical access to the JBC and cables.
The JBC has a button used to close the polls. It is possible but not required to password protect this function. If the polls are closed, all DREs attached to the JBC would be closed. There is a risk that an unauthorized person could close the polls prematurely.	We recommend the Secretary of State require that Hart InterCivic incorporate mandatory user passwords of at least six characters in length for closing the polls using the JBC. We also recommend the Secretary of State require that Hart InterCivic incorporate a warning prior to closing the polls before the scheduled end of the election. We also recommend the Secretary of State require that administrative policies and procedures be put into place regarding access to the JBC.

Election policies and procedures have long been used to ensure fair and accurate election results. The deployment of DRE technology will not lessen the need for well thought out and consistently enforced policies and procedures.

PART FIVE: SEQUOIA

Overview

This section details the assessment for the Sequoia AVC Edge DRE. The AVC Edge is a Touch Screen Voting System. Navigation within the ballot is accomplished with scroll buttons to move forward and backward, and the Contest Box, which enables voters to move to any part of the ballot. Voters can verify their selections and change their vote at any time before they cast their ballot.

The AVC Edge has an LCD touch-screen with large typeface. Wheelchairs are accommodated by adjusting the screen's height. No other adjustments are necessary. The Audio Voting feature allows the AVC Edge to serve blind voters and people who have difficulty reading. Ballots in multiple languages are available on the Edge. Allowing a voter to simply choose the preferred language on the first screen, the ballot is then presented in that language until the voting process is complete.

The AVC Edge is supported by the WinEDS Election Management software, which provides ballot creation, vote tabulation, and reporting.

The AVC Edge prevents the voter from overvoting, notifies the voter of undervoting, and allows the voter to review and modify their ballot choices before casting their vote.

Compuware tested the following hardware and software in this technical security assessment:

Hardware	Software
• AVC Edge version 4.1. D • Card Activator version 4.2	• WinEDS Election Management Software version 2.6

Step 1: Characterization of the AVC Edge Voting System

In Step 1, the AVC Edge was examined for the following:

- AVC Edge system interfaces – input/output connections between the AVC Edge and external entities, and the related voting processes
- Work flow / process model – flow of data through the AVC Edge system interfaces, and the related voting processes
- AVC Edge environment
    - Hardware configuration
    - Software configuration
    - Network configuration

AVC Edge System Interfaces

The following diagram provides a graphical overview of the connections to the AVC Edge. The diagram shows the input/output connections between the AVC Edge and external entities such as the BOE's and voters.

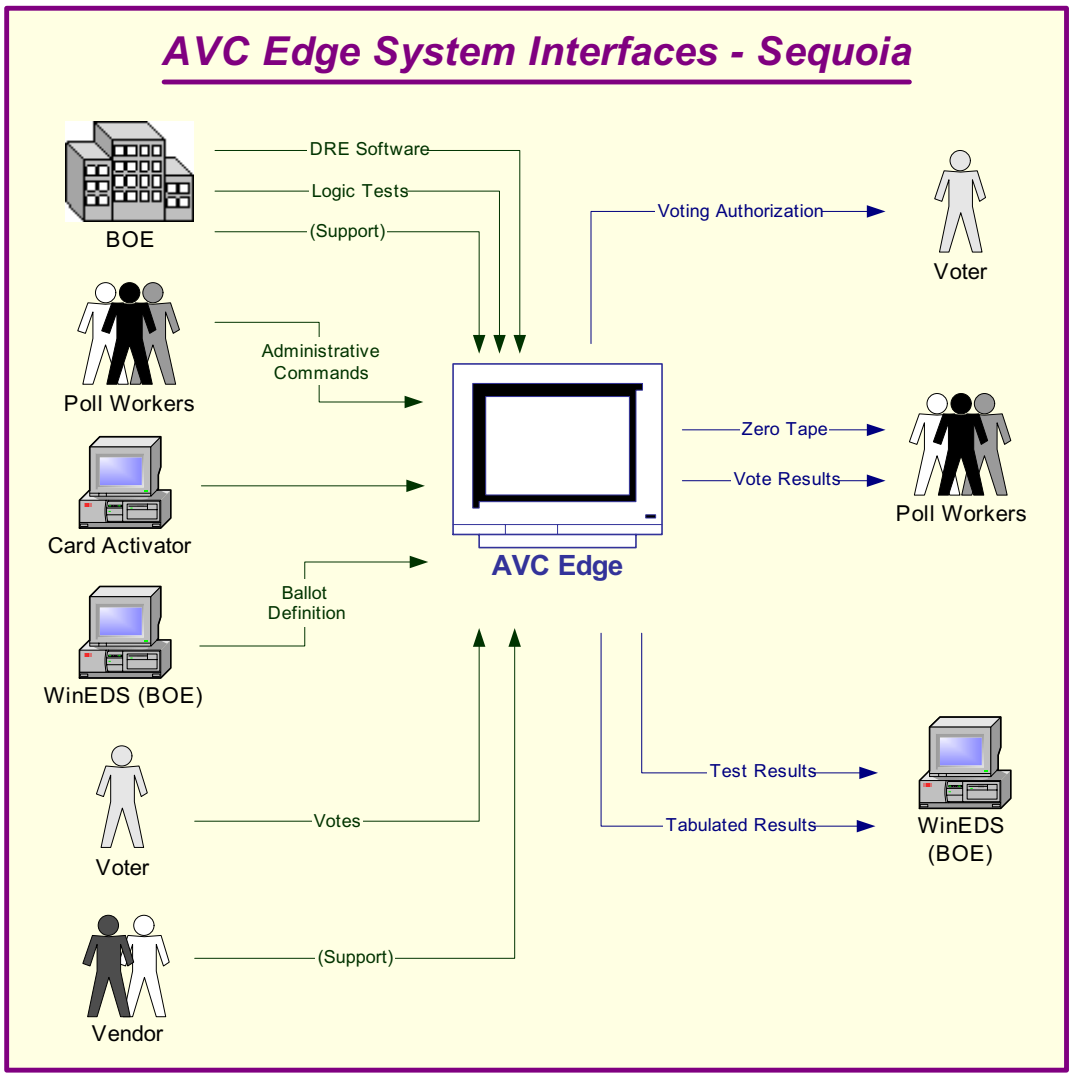

Figure 11 – *AVC Edge System Interfaces - Sequoia*

Continued on the next page

AVC Edge System Interfaces (continued)

Following is an explanation of the tasks related to the AVC Edge system interfaces.

Inputs	Outputs
Board of Elections	
• The WinEDS Election Management Software is installed on a computer at the Board of Elections (BOE). • The BOE uses WinEDS to create the ballot definition that is loaded to the AVC Edge.	
• Workers at the BOE enter data into the AVC Edge to perform the logic and accuracy testing (LAT). • If there is a problem, the BOE troubleshoots the problem and determines if county workers can solve the problem or if the vendor needs to be called.	Workers at the board verify the results that were entered in the LAT.
Vendor	
If there is a problem with the LAT, the vendor may be called in to repair the unit. If the unit is repaired, it must successfully go through the LAT before it may be used in an election.	
Poll Workers	
• Poll workers set up the booth. • Poll workers open the AVC Edge for voting. • Poll workers authorize the voter to vote.	Poll workers print a zero tape from the AVC Edge to ensure there are no pre-existing votes recorded on the unit.
Voter	
• Voter takes the authorization to the AVC Edge, which presents the correct ballot to the voter. • Voter votes the ballot. The AVC Edge prevents the voter from overvoting, notifies of undervoting, and presents the ballot choices for review as appropriate.	
Poll Workers	
	• Poll workers print result tapes from the AVC Edge. • Poll workers post one result tape at the precinct. • Poll workers remove the PCMCIA card and send the card and a copy of the result tape to the BOE.
Board of Elections	
	• The BOE places the PCMCIA card from the AVC Edge into a media reader, and the WinEDS software counts the votes. • The BOE prints and releases the results.

Work Flow / Process Model

The following diagram provides a graphical overview of the work flow associated with the AVC Edge system interfaces, and represents the next level down from the Context Diagram. This diagram displays the flow of data through the AVC Edge system interfaces.

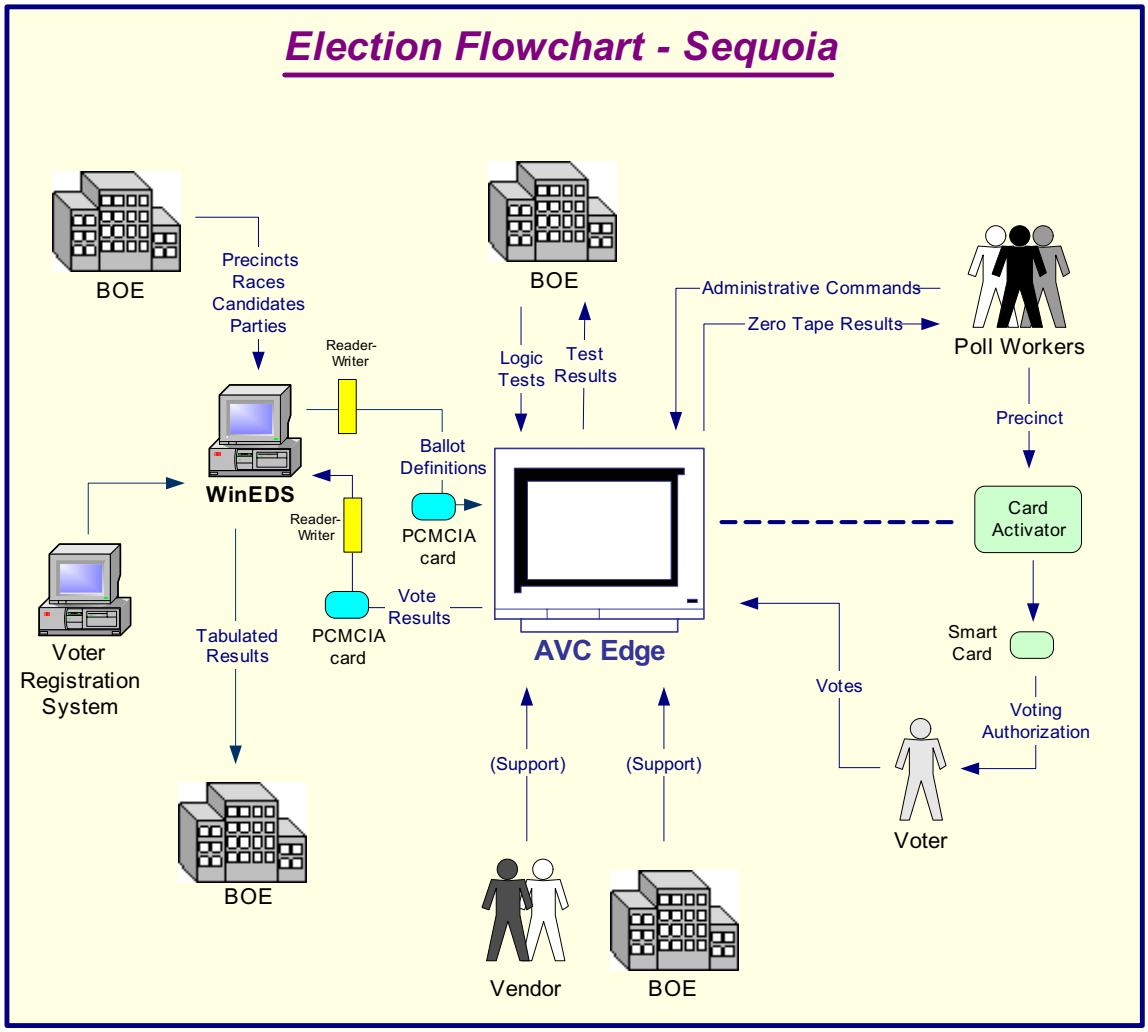

Figure 12 *– Election Flowchart - Sequoia*

Continued on the next page

Work Flow / Process Model (continued)

Following is an explanation of the work flow associated with the AVC Edge system interfaces.

Inputs	Outputs
Board of Elections	
• The WinEDS Election Management Software is installed on a computer or on a closed network at the BOE. • Precincts are entered into the WinEDS software either by data entry or by loading from the county voter registration system. • Races are defined in the WinEDS software and related to the precincts. • Candidates are entered into the WinEDS software and related to the races. • The BOE uses the WinEDS software to create the ballot definition by writing the information to a PCMCIA card. • A copy of the database is transferred to the Tally software.	
• Workers at the BOE enter data into the AVC Edge to perform the logic and accuracy testing (LAT). • If there is a problem, the BOE troubleshoots the problem and determines if county workers can solve the problem or if the vendor needs to be called.	Workers at the BOE verify the results that were entered in the LAT.
Vendor	
If there are problems with the LAT, the vendor may be called in to repair the unit. If the unit is repaired, it must successfully go through the LAT before it may be used in an election.	
Poll Workers	
• Poll workers set up the AVC Edge vote booth. • Poll workers open the AVC Edge for voting. • Poll workers authorize the voter to vote by issuing the voter a smart card.	Poll workers print a zero tape from the AVC Edge to ensure there are no pre-existing votes recorded on it.
Voter	
• Voter enters the smart card into the AVC Edge, which then displays the correct ballot for the voter. • Voter votes the ballot. The AVC Edge prevents the voter from overvoting, notifies of undervoting, and presents the ballot choices for review as appropriate.	

Continued on the next page

Work Flow/Process Model (continued)

Inputs	Outputs
Poll Workers	
	• Poll workers print the result tapes from the AVC Edge. • Poll workers post one result tape at the precinct. • Poll workers remove the PCMCIA card and send the card and a copy of the result tape to the BOE.
Board of Elections	
	• BOE places the PCMCIA card from the AVC Edge into a media reader, and the WinEDS Tally feature counts the votes. • The BOE prints and releases the results.

Environment

Hardware Configuration

Following is a summary of the hardware configuration of the Sequoia AVC Edge that was tested.

Processor Type	Processor Clock Speed	Memory	Operating System	Communications Slots	Input Interfaces
National Semiconductor Geode GX1	200 - 333MHz	• 32MB Compact Flash – internal • 64MB DRAM • No hard disk	DOS compatible	• PCMCIA cards/slots	• Serial port on card activator • 2 PCMCIA slots • 1 smart card slot

Software Configuration

Following is a summary of the software configuration of the Sequoia AVC Edge that was tested.

Firmware	User Interface	Internal Storage	Communications Protocols	Security
DOS compatible	Proprietary GUI software displayed on push button LCD screen.	The data is stored in binary format in the PCMCIA card and AVC Edge internal memory.	Has PCMCIA card slots.	Voters can access AVC Edge device using the smart card, which is activated by the Card Activator.

Network Configuration

There is no network-based LAN\WAN connection between the DRE and the Voting Software that resides on a Windows-based machine. The only network connection that could exist is between the voting machine and central voting software. Only if the county chooses to send the accumulated votes from the polling location to the tabulating location would a dial-up connection or network connection be used.

For the scope of this project we are not reviewing any connections outside the DRE, such as dial-up connections or network connections leading to the tabulation of votes.

Step 2: Threat Identification

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. Vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised. In determining the likelihood of a threat, one must consider threat-sources, potential vulnerabilities (Step 3), and existing controls (Step 4).

In Step 2, the assessment team determined the potential threats posed to the AVC Edge voting system. Following is a list of potential threats to which the AVC Edge voting system could be exposed.

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Campaign and political entities	Competitive advantage Economic espionage Change outcome of election	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Step 3: Vulnerability Identification

The analysis of the threat to an electronic voting system must include an analysis of the vulnerabilities associated with the system environment. In Step 3, the assessment team identified vulnerabilities (flaws or weaknesses) of the system. Results from audits, tests, inspections, and an examination of the current state of the AVC Edge voting system were used to determine existing weaknesses.

The assessment team conducted a comprehensive review of compliance to both technical and non-technical requirements to identify vulnerabilities. In addition to identifying weaknesses in the above, the team also assessed external entities and their connectivity to the AVC Edge voting system.

Requirements Tested & Test Results

This section documents the requirements that were tested, the tests conducted, and the results of each test.

Test Areas

Tests were conducted in the following areas.

1. Code Review Tests
2. Platform Review Tests
3. Physical Tests

Specific Tests and Test Results

The assessment team tested the specific scenarios listed below. For each scenario, the table lists:

- Description of the requirement tested
- Test Scenario that covered the requirement
- Test Results

No.	Requirement	Test Scenario	Test Results
Code Review			
Standardization - Naming conventions of variables, constants and modules should be consistent across the application. Construction of modules within an application should also be consistent. This is important for knowledge transfer and code maintenance.			
1.01	There shall be a standard method in the naming functions and variables.	Perform visual review of source files. Function names will be checked for proper case formatting of concatenated words. Names of functions should clearly describe its purpose.	Upon review of the code, it is noted that proper case formatting is used for function names and the names describe the purpose of the function.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
1.02	There shall be standard method in the construction of modules.	Perform visual review of source files. Modules should contain a consistent format and location for module components. Modules should begin with comments describing the modules contents. Location of methods and variables with associated comments should be consistent throughout.	Modules use a consistent format for comments and location of variables and methods. An exception is in the WinEDS 2.6 code, where comments were found to be limited to code blocks only.
Coding Conventions - The application should be broken down into modules with each module performing a single function. There should be single entry and exit points within a module. There should be consistent error handling throughout the application. Naming of variables, constants and modules should be descriptive and self-explanatory.			
1.03	There shall be a standard methodology used for the construction of modules.	Perform visual review of source code. Modules should use a clear methodology of construction. Files will be reviewed to see if a coding industry standard is used in the naming of modules, functions, variables and constants.	Code follows an "industry" standard methodology in naming of modules, functions, variables and constants.
1.04	The naming of variables and functions shall be clear and descriptive.	Perform visual review of source code. Function and variable names should be "self documenting" as well as contain properly typed and sized attributes, and return types.	The function and variable names are self-describing and proper attribute and return types are used in the code.
1.05	There shall be a consistent way to handle system errors.	Perform visual review of source code for implementation of error handling code. All methods should contain error-handling logic. Systems should remain stable in the event of an error. When an error occurs, sufficient information regarding the state of the system and system parameters should be recorded for future debugging.	Upon review of the code, it is noted that proper error-handling procedures are implemented and appropriate messages/beeps are returned in the event of an error. The audit trail logs the important events in the results cartridge and the internal memory of the AVC Edge.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
Code Documentation - All source code should be sufficiently commented, with clear descriptions of what is being accomplished by each module, the names of calling functions, and the inputs and outputs to the modules. Consistency should be maintained in commenting the code for ease of readability.			
1.06	The comments in the code shall be descriptive and present in the code.	Perform visual review of source code. Comments will be reviewed for simple descriptive content. Comments should appear at the beginning of each module, function. All module level variables, constants, and structures should be commented as well. Function parameters and return values should describe appropriate values. Comments should also appear in methods to help clarify complex code and logic behind expressions.	Upon review of the code, modules have comments at the beginning and comments are available for variables, constants, structures and complex logic. An exception is the WinEDS 2.6 code, which does not have comments at the beginning of each module. This application utilizes the PFC and these modules have header comments as originally provided by Sybase. The only comments found are for logical blocks of code.
1.07	The comments shall have a consistent look in their layout.	Perform visual review of source code. Comments should have a common format with standard fields for information. Some standard fields should be a description, parameters, return types, a change log.	A common format for comments is followed, with the following standard fields: description, parameters, return types and change log. An exception is the WinEDS 2.6 code, which does not have comments at the beginning of each module. This application utilizes the PFC and these modules have header comments as originally provided by Sybase. The only comments found are for logical blocks of code.
1.08	The modules shall be commented describing their contents.	Perform visual review of source code. Modules should have a standard comment identifier at the beginning of each module. Module comments should contain the name and description of the module, a copyright notice, and a change log.	Upon review of code, module comments contain name, a brief description of the module purpose, copyright notice and a detailed change log. An exception is the WinEDS 2.6 code, which does not have comments at the beginning of each module. This application utilizes the PFC and these modules have header comments as originally provided by Sybase.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
1.09	There shall be a close relationship of the requirements to the code modules that implement the requirements.	Perform visual review of the source code. Modules will be reviewed for their functional content. The variables and functions should be closely related and work directly to perform a clear task.	Code is available in the modules perform the specified tasks and unused variables/code was not found.
Coding Complexity - Code should be simple in construction. It should be easy to read and follow. Modules should perform single tasks and should have single points of entry and exit.			
1.10	The system shall be divided into modules.	The source code will be visually reviewed to verify if the code has been properly modularized. Modules should be an appropriate length and encapsulate related functionality.	Several modules with appropriate lengths have been created in the project.
1.11	The source code shall use simple logic structures.	The source code will be visually reviewed for the use of simple and clear logical structures. There should be the use of constants (consts) and data structures (structs) to improve code readability and reliability.	Constants and data structures are used consistently in the system to improve readability and reliability.
1.12	The source code shall have an appropriate size of modules and the number of functions performed by them.	The source code will be visually reviewed to verify if the code has been properly modularized. Modules should encapsulate related functionality into logical groupings with clear interfaces. Interfaces should be well defined as to their use.	Upon review, it is noted that the code is properly modularized and the module size is managed correctly by implementing necessary functionality only.
Classes / Modules - Use of classes / modules can make the code smaller and reusable.			
1.13	There shall be the existence of classes and modules.	The source code will be visually reviewed to verify implementation of classes and proper modularization of the source files.	Most of the AVC Edge software is written in C. Since C does not implement classes, they have not been used. But proper modularization of code is done.
1.14	The functions performed by the classes shall be self contained where appropriate.	The source code will be visually reviewed. The name and description of the class should be simple and clear. The task performed by the function should be easy to understand, simple to define, and atomic.	As noted above, the code has many modules and each implements a specific functionality. The module size makes the code readable and easy to understand.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
Third Party Components - Use of third party components requires strict guidelines, security standards and version control. Attention will be paid to controls around third party components used in the applications.			
1.15	Any use of third party components in the firmware shall be inspected.	The source code will be visually reviewed to find any use of third party products. The makers and the versions of any found third party applications will be noted.	The following third party softwares are used in AVC Edge system: Phoenix BIOS, Metagraphics graphics functions, Menuet windowing system, Flash File System for ATA style PCMCIA flash ROM and CompactFlash.
1.16	Any third party components shall be secure and not create a risk.	If the source is available for any used third party products, the source will be reviewed for client modifications. Third party source code should only contain the necessary functionality with unused areas removed or disabled. If the source is not available then further study will be required.	A specific boot code for the AVC Edge start up is used in the firmware. On review, it is noted that the third party software only provides specific functionality needed for AVC Edge system to function. Firmware updates are done using specially configured cartridge and a password to validate the cryptographic signatures on the files to be updated.
Database Review - Database integrity and data security is vital for correct data reporting. The code review will include the following:			
1.17	The database shall be well designed.	The data model and database source code will be reviewed for existence of proper keys and normalization.	No database is used in the AVC Edge. Data files are stored in the results cartridge and resident memory of AVC Edge in proprietary format.
1.18	The data in the database shall be secure.	The source code will be visually reviewed for user access levels and roles implemented as part of security in SQL Server 2000.	Not applicable to the design of AVC Edge.
Data Integrity - Review the internal data storage of the system using the following criteria:			
1.19	There shall be ways to verify the correctness of system data.	Source code will be reviewed and tested in order to check for CRC/Checksum techniques in verifying the correctness of data that is stored in memory. Can the software identify data that has been improperly modified?	CRC 16 algorithm has been implemented in the code to check for the correctness of the ballot image. Multiple read–write operations are implemented to make sure the data has not changed. This is done between each vote and power up.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
1.20	There shall not be any means by which a voter can be identified.	The source code will be reviewed to make sure that an algorithm is implemented to make sure voter records are stored in random order. The vote records should not have time stamp associated with it.	The vote records are stored in a random order in the results cartridge. A pseudo-random number generator (a 32-bit maximal length random sequence is seeded by the seconds portion of the internal clock) is implemented in the code.
1.21	The system shall be secure and prevent any access other than from authorized voters or supervisors.	The source code will be reviewed to verify the system is secure and allows each voter to only vote once.	The smartcards used by voters are kept valid for a certain timeframe. Logic is implemented to de-activate the card by putting random data once it is used to enter a vote. Using the same card (without activation) gives a visual error message.
1.22	There shall be a system to protect and backup data in the event of a disaster.	The source code will be reviewed to verify there is a means by which votes can be recovered incase of a system disaster.	Recorded Votes and audit logs are stored in redundant memories (the internal memory in the AVC Edge and the results cartridge). In case of data mismatch, a consolidation card can be created from WinEDS software and used to read results from the AVC Edge.
Encryption Standards - Review of encryption standards used in the DREs and the supporting software will be a point of primary focus while the source code is being reviewed.			
1.23	There shall be a strong method of encryption used.	The strength of encryption will be reviewed. The types of encryption will be reviewed to see if it is sufficient.	The type of encryption used is DES (Data Encryption Standard) signed with SHA-1 (Secure Hash Algorithm). The cryptographic key appears to be derived from the hard-coded seed 1024 (refer to EEPROM_SZ in file Edgemap.h).

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
1.24	The data shall be encrypted including "*ballot definitions*" and other data on the DREs.	Ballot Definitions and Cast Vote Records should be protected and be verifiable they are correct. Encryption should be powerful enough to block access to stored data.	On examining the code, it is noted that the ballot definition and cast votes are not encrypted. At the time of closing the polls, cryptographic signatures are calculated and stored for each of the totals data files. These signatures are stored in both the audit trail and results cartridge.
1.25	There shall be the use of cryptographic operations during voter authorization.	Various means of "voter identification" should be secure. The data on a voter authorization smart card should not be discernable.	The voter smart card is encrypted using DES signed with SHA-1.
1.26	There shall be the use of encryption keys protecting types of removable media. Those keys shall be protected during the transportation of Ballot Definitions and Voting Records.	Encryption keys should be randomly generated every time and sufficiently long so that it is not easy to guess. The code will be reviewed to see if the keys are used in smart cards and PCMCIA cards.	Encrypted keys are not used in the results cartridge (PCMCIA card). The contents of the voter smart card are encrypted using DES and signed with SHA-1.
1.27	Any data transmitted shall be encrypted over communication links.	Transmission protocols will be checked for the use on encryption. Data should never travel over a wire without protection. The contents of the transmission should be verifiable as to their contents and correctness. Any type of tampering should be identifiable if not impossible.	The AVC Edge system is not on a network. At the poll location, the results cartridge is inserted into the AVC Edge and the vote data and audit trail information is stored in the cartridge and internal memory of AVC Edge unit. At close of polls, the results cartridges are physically transported to computer(s) at central location and are read by the WinEDS software to tally the results.
1.28	The AVC Edge shall not have unencrypted cast ballot records.	Check the vote records on the AVC Edge, WinEDS software, and transfer medium to ensure that the records are encrypted.	The vote records and ballot information are not encrypted. Cryptographic signatures for each of the totals data files (ballot images, selection code summary totals and candidate summary totals) are computed and stored in the AVS Edge and results cartridge.
1.29	The AVC Edge shall not have unencrypted audit logs.	Check the audit logs on the AVC Edge to ensure that they are encrypted.	Upon review of the code, it is noted that the audit log information in the AVC Edge or results cartridge are not encrypted.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
1.30	The system shall not store or use passwords without encryption.	Perform code review to ensure that passwords used in all software are encrypted.	The AVC Edge does not require passwords during an election process. Passwords are required only while updating the firmware software. Based on the code, the technician password is in an encrypted database file. This file is not available for review.
1.31	The system shall not use hardcoded passwords.	Perform code review to ensure that the system does not use hardcoded passwords.	On review of the code, hardcoded passwords were not found in the AVC Edge code.
Platform Review			
2.01	The AVC Edge shall not allow supervisor privileges to unauthorized individuals.	Use the yellow button on the back of the AVC Edge to enter supervisor mode.	The AVC Edge enters supervisor mode without entry of any password or other security measures. Any voter could place the AVC Edge in supervisor mode in a few seconds.
2.02	The system shall not allow unauthorized modification of the Ballot Definition file.	Try to modify the Ballot Definition file on the PCMCIA result card before loading it on the AVC Edge.	We were able to read and modify portions of the Ballot Definition binary files on the PCMCIA card, but the system read the changed files as bad and would not load them onto the system.
2.03	The AVC Edge shall not allow the installation and/or execution of an unauthorized program.	Install a program on a PCMCIA result card, insert it in the AVC Edge, and install and/or execute the unauthorized program.	The system did not load the unauthorized program from the PCMCIA card into the AVC Edge. It identified a bad file on the card and asked for the card to be removed. This test was run using an executable and a self-extracting executable file.
2.04	The system shall not allow for security breaches via the network.	Inspect the AVC Edge for network accessible ports.	The system contains an RS-232 serial port used for printing. The system also contains two PCMCIA slots. The card activator contains a 9 pin serial port.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
2.05	The system shall not allow for security breaches via the internet.	Try to access, modify, or disrupt the functioning of the AVC Edge software while connected to a network.	Attempts to manipulate the AVC Edge using a PCMCIA modem card attached to the PCMCIA slots resulted in an error message indicating the card was not recognized. No manipulation was possible.
2.06	The AVC Edge shall be resistant to tampering, lock up, intrusion or vandalism.	Try to bring the system down, lock up the operating system, change or erase log files, or any other form of Denial of Service (DoS), Distributed Denial of Service (DDos), or other result which benefits the attacker.	Attempts to disrupt the system failed. The system did not load the unauthorized program from the PCMCIA card into the AVC Edge AVC Edge.
2.07	The AVC Edge shall not allow supervisor privileges to unauthorized individuals.	Try to gain admin rights or system rights using the switches and controls on the unit.	An election can be closed on the AVC Edge by turning a switch on the back of the unit from the open position to the closed position. This switch can have a wire seal for protection. As an option, this switch can be ordered as a keyed switch. Sequoia also provides an optional feature to prevent poll closure until a scheduled time. This option was not tested during the evaluation. There is no password or confirmation entry requested during closure. Supervisor rights can be gained by using the Activate button on the back of the AVC Edge once the polls are closed.
2.08	The operating system on the AVC Edge shall be hardened against unintended intrusion, operations, or forced errors.	Try to cause a kernel panic, system failure, or indefinite wait state, or other operating system lock-up within the operating system or sub-system.	Attempts to disrupt the system failed. The system did not load the unauthorized program from the PCMCIA card into the AVC Edge AVC Edge.
2.09	The system shall password protect supervisor functions.	Observe that functions are password protected, the minimum length of passwords, and that they can be changed.	Supervisor functions are not password protected.
2.10	The system shall not allow corruption of the O/S, application program, ballot definition, or voter data.	Try to create an attack on flash memory using files loaded on the PCMCIA result card.	The system would not read files from the PCMCIA card and read them as bad files on the card.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
2.11	The system shall not allow undetected tampering with or modification to the contents of removable media.	Change the contents on a result media card and use the card. Determine if the system reports the card has been modified.	The system would not read files from the PCMCIA card and read them as bad files on the card.
2.12	The AVC Edge shall maintain a protective counter of the total number of votes cast in all elections.	Try to modify protective counter.	There is no way to access the protective counter through menus, ports, the PCMCIA card, or other means.
2.13	The AVC Edge shall not allow "Man-in-the-middle" attacks when communicating between the Election Management software and the AVC Edge.	Observe the hardware and communication architecture to determine if such attacks are possible.	The AVC Edge is not on a LAN\WAN network and does not dial out over a phone line. Man-in-the-middle attacks are not possible.
2.14	The AVC Edge shall protect all COM ports from intrusions or vulnerabilities.	Try to gain access via an open TCP/UDP or serial or USB or other port.	There are no COM ports that will respond to an intruder. The printer serial port communicates one way.
2.15	The AVC Edge shall be resistant to introduction of Trojans, viruses, or any other form of malware.	Try to introduce any type of malicious software (malware) into the system.	We were unable to load any type of malware into the AVC Edge. The system did not load the unauthorized program from the PCMCIA card into the AVC Edge.
2.16	The system shall have a programmable memory device that is sealed in the unit with means of tamper detection.	Inspect the hardware design documents and physical hardware.	The PCMCIA cards are loaded behind a plastic door that can be sealed with a wire seal. Anyone tampering with the cards would need to break the seal.
2.17	The system shall provide for safeguards against and evidence of tampering, theft or damage of the system and units.	Inspect the physical hardware for location of seals and locks.	The storage case does not have provisions for locks or seals. Only the internal seals attached to the PCMCIA case would provide evidence of tampering while the system was in storage or transported to an election.
2.18	In the event of the failure of a unit, the system shall retain a record of all votes cast prior to the failure.	Start voting on the AVC EDGE, and then disconnect batteries for 30 minutes to simulate a power outage. Resume power and start up the AVC EDGE, and check the voter information.	Once the AVC Edge batteries are drained to a critical level, the AVC Edge discontinues voting and shuts down. Once power is restored, voting can be resumed and no votes or audit information are lost.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
Physical Testing			
3.01	There shall be a programmable memory device sealed in unit with means of tamper detection.	Check PCMCIA card to determine whether it can be removed easily and can be locked.	PCMCIA card is housed in a locked compartment and is not easy to remove when locked.
3.02	Poll opening reports should have all system audit information required.	Conduct logic and accuracy tests and verify system audit information is present.	Logic and accuracy tests were conducted before the election. System audit information is displayed on the resulting print out.
3.03	The system shall store logic and accuracy test results in memory of the main unit processor and Election Day device.	Conduct logic and accuracy test and verify results are recorded in the on-board memory by printing the audit log.	Logic and accuracy tests were conducted before the election to verify system information was correct. Logic and accuracy test result were printed in the audit log.
3.04	The system shall provide logic and accuracy tests in the memory of the main processor and the programmable memory device used on Election Day, including zero printouts before each election and a precinct tally printout at the close of each election.	Conduct logic and accuracy testing before election is started. Print a zero tape before an election and a result tape after an election.	Logic and accuracy tests were conducted before the election to verify counters are working properly and the programming for each voting device is correct. A zero tape printout was created and verified that no votes were cast before the start of the election. After voting was closed, a result tape was printed.
3.05	The system shall control logic and data processing methods to detect errors and provide correction method.	Create an instance where a known error will occur on the AVC Edge. For instance, enter a voter card after it has been de-activated.	AVC Edge displays a concise error message. This is standard throughout all error handling functions on the AVC Edge.
3.06	The AVC Edge shall provide a mechanism for executing test procedures which validate the correctness of election programming for each voting device and polling place and insure that the ballot display corresponds with the installed election program.	Conduct a logic and accuracy test.	Logic and accuracy tests were conducted before the election to verify counters are working properly and the programming for each voting device is correct.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.07	The EMS software shall not allow unauthorized modification of the Ballot Definition data.	Try to modify the Ballot Definition in the WinEDS software using a database viewer/program.	WinEDS uses an MS SQL Server 2000 database. The Database sever contained an ODBC connection to the SQL Server database. Using MS Access from the administrator account, we were able to connect to the election results database and modify the data from the election. When connecting to the database with access, we enabled the "trusted connection" check box. We were also able to open the SQL Enterprise Manager without a password and modified the data.
3.08	The system shall present the ballot to the voter in a clear and unambiguous manner.	Create an election ballot definition file and transfer the file to the AVC Edge. Open election and look at ballot.	The ballot is presented in a clear and unambiguous manner.
3.09	The AVC Edge shall not allow voters to vote multiple times.	Insert an authorized smart card into the AVC Edge voting machine and try to use it to vote multiple times.	Once a vote has been cast, the smart card used is deactivated. When trying to insert the deactivated smart card to vote again, the card is retained in the card reader.
3.10	The AVC Edge shall not allow voters to vote multiple times.	Insert a counterfeit smart card into the AVC Edge and try to use it to vote.	We were unable to manufacture a counterfeit voter card. Using an ACR80 Card Tool purchased on-line we were not able to read or write information onto the voter smart card and all attempts to manufacture a smart card were defeated.
3.11	The system shall not allow voting access to unauthorized persons.	Create a counterfeit Voter Access smart card then attempt to use it so it is recognized and authenticated by the AVC Edge voting machine.	Unable to manufacture a counterfeit voter card. Voter card could not be read by the smart card reader.
3.12	The AVC Edge shall not allow viewing or changing vote results during the election process.	Access the supervisor screen and try to change the voting results during the election process.	The supervisor screen does not have the functions to change the vote results. Only the manual voting option and printing option for Zero tape are displayed if the polls are open.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.13	The AVC Edge shall not allow the accidental or unauthorized closing of the election.	Access the supervisor screen and try to close the election.	The supervisor screen does not have the function to close the election. Turning the switch behind the AVC Edge to "Close polls" can close the election.
3.14	The AVC Edge shall not allow the accidental or unauthorized reset of the AVC Edge.	Access the supervisor screen and try to reset the AVC Edge.	The supervisor screen does not have the function to reset the AVC Edge after election process begins. But the Power OFF switch is accessible to the voter and can be turned off though this does not affect the voting process. When powered back ON, the AVC Edge starts up where the power was turned OFF. Once the polls are closed, the supervisor screen can reset the AVC Edge.
3.15	The AVC Edge shall not allow the use of an unauthorized PIN to access supervisor functions.	Access to supervisor screen using a PIN.	The AVC Edge allows access to the Supervisor screen without a PIN. The access is granted by a selection of special keystrokes.
3.16	The AVC Edge shall not lose voter information, vote count, Ballot Definition information, etc. due to a power outage during the election.	Start voting on the AVC EDGE, and then disconnect power for thirty minutes to simulate a power outage, and then resume power. Cast votes before, during, and after the disruption.	Power switch is easily accessible and when power is turned off, votes cast are still in system, but current voter must re-vote. The results of the previous votes are not lost and are stored in the AVC Edge and the PCMCIA card.
3.17	The AVC Edge shall not lose voter information, vote count, Ballot Definition information, etc. due to a power outage during the election.	Start voting on the AVC EDGE, and then disconnect batteries for 30 minutes to simulate a power outage. Resume power and start up the AVC EDGE, and check the voter information.	Once the AVC Edge batteries are drained to a critical level, the AVC Edge discontinues voting and shuts down. Once power is restored, voting can be resumed and no votes or audit information are lost.
3.18	The AVC Edge shall not allow for modification of the "protective counter" which tracks the total number of votes cast on the machine.	Try to modify the protective counter on the AVC EDGE.	Supervisor functions will not allow the altering of counts on the AVC Edge voting machine. Counter is stored within the CPU on the AVC Edge. The number on the counter is printed out before the election and after the election as well.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.19	The AVC Edge shall not allow modification that forces it to use the same storage device for all of the data.	Modify the AVC Edge so that only core flash memory is available and see if the system will allow voting.	The AVC Edge will not operate unless removable flash memory is present in the existing slot. The AVC Edge displays an error message and does not allow any activities to take place until the card is inserted back into the AVC Edge.
3.20	The system shall not allow supervisor access to unauthorized persons.	Try to access the supervisor screen.	The AVC Edge allows access to supervisor screens with the use of a combination of special keystrokes.
3.21	The audit logs shall record all instances of supervisor access to the AVC Edge.	Review audit log after completing successful vote test and ensure each step that used supervisor access is correctly logged.	Audit log is complete and accurate. It records all actions by the Supervisor on the AVC Edge.
3.22	The system audit log shall contain sufficient information to allow the auditing of all operations related to central site ballot tabulation, results consolidation, and report generation. It shall include a/an: • Identification of the program and version being run • Identification of the election file being used • Record of all options entered by the operator • Record of all actions performed by the subsystem • Record of all tabulation and consolidation input	Print a copy of the audit log and verify all items are recorded.	Audit log was printed and all information listed in requirement was printed and verified.
3.23	The system audit log must be created and maintained by the system in the sequence in which operations were performed.	Print a copy of the audit log and verify all steps are recorded sequentially.	The audit log is generated in sequential order and each transaction within the audit log is time stamped.
3.24	The system audit log must be created and maintained by the system in the sequence in which operations were performed.	Review audit log after completing successful vote test and ensure each step that used supervisor access is correctly sequenced.	The Audit log records all the actions on the AVC Edge in the sequence in which the operations were performed.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.25	The system shall provide for safeguards against and evidence of tampering, theft or damage of the system and units.	Review audit logs to verify any act will be recorded and logged with a timestamp.	All actions to the AVC Edge are recorded in the audit log with a time stamp. This includes opening and closing the polls, voting, inserting invalid voting cards, loss of power, and supervisor access.
3.26	The media/medium in which vote counts are transferred to the Tally software shall not allow modification of the vote count.	Try to access and modify the vote count on the PCMCIA before the vote count is loaded into the WinEDS software.	We were unable to alter vote counts on the PCMCIA card, which stores the data. After modifying the contents on the PCMCIA card, the WinEDS software doesn't recognize the PCMCIA card with the results.
3.27	The system shall ensure that a voter's exact voting record cannot be traced back to the voter.	Try to access the information needed to reconstruct a voter's exact voting record.	The Audit reports and the Summary reports from the AVC Edge cannot recreate the voters exact voting record. The supervisor screen does not have the function to view the exact voting records of each voter. The system will provide for provisional voting by creating a sequence to list provisional voter records.
3.28	The system shall prevent modification of the voter's vote after the ballot is cast.	Verify vote cannot be altered once the ballot has been cast.	User cannot alter vote ballots cast. There is no supervisor function to allow for the votes cast to be altered.
3.29	The system shall protect the secrecy of the vote such that the vote may not be observed during the voter's selection of preferences, during the casting of the ballot, and as the voted ballot is transmitted for recording on a storage device.	When the vote is being cast, others should not be allowed to view the voter's selection of preferences.	There are no supervisor functions to allow the view of a voter's selection. The supervisor must close the election to print reports. Curtains protect the voting booth.
3.30	The system shall prohibit voted ballots from being accessed by anyone until after the close of polls.	Verify reports can only be executed after the polls have been closed.	Reports can only be created when polls are closed. The Print option is enabled once the switch is turned to "Close Polls".

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.31	The system shall provide that each voter's ballot is secret and the voter cannot be identified by image, code or other methods.	Conduct a mock election and try to trace votes to a voter.	The system does not allow any access to identify the Voter. The supervisor screen does not have this capability. After closing polls, the screen displays to print the summary report but does not provide the means to identify a voter with his/her ballot. Provisional voting is handled differently. Voter records can be re-constructed to verify if the vote cast is allowed or not allowed.
3.32	The system shall provide a summary screen at the end of the ballot showing what the voter has chosen prior to the final vote being cast.	Vote for all issues and/or candidates and before casting the ballot, verify a summary of all votes is presented.	A summary of all votes for each race for the particular user is displayed before we can cast the ballot. Corrections to any race can be made at this point.
3.33	The AVC Edge shall not allow unauthorized modification to its operating system.	Try to modify the operating system on the AVC Edge by loading a new operating system off the PCMCIA card.	Attempted to load a counterfeit program using the PCMCIA card. The Program loaded into PCMCIA card was not recognized and was not loaded into the AVC Edge.
3.34	The AVC Edge shall not allow printing of summary reports before the sequence of events required for closing of the polls are completed.	As a Supervisor, print reports before closing the election.	Until the switch is turned to "Close Polls" the AVC Edge doesn't give the option to print summary reports. The supervisor screen also does not have the Summary screen report option prior to closing the polls.
3.35	There shall be no loss of data during generation of reports including results, images and inaccurate vote counts.	Print out reports after election has been closed and verify no inaccuracies exist.	Printed election reports after the close of the election and verified no results were lost during this function.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.36	The system shall provide printed records regarding the opening and closing of the polls and include the following: • Identification of election, including opening and closing date and times • Identification of each unit • Identification of ballot format • Identification of candidate and/or issue, verifying zero start • Identification of all ballot fields and all special voting options • Summary report of votes cast for each device, or ability to extract same	Close the election and print out a copy of the audit log and review all transactions.	All transactions are captured on the audit logs including specific information about the AVC Edge, definition of the election, and all actions occurring on the AVC Edge during the election. All items identified in this requirement are present.
3.37	The system shall produce a paper audit trail. To guard against fraud, systems shall not produce individual paper records that voters could remove from the polling place.	Complete and close an election and print out a copy of the audit log from a specific AVC EDGE.	An audit log is printed out using a specific supervisor function. The audit log produces a report that is a paper trail to guard against fraud.
3.38	The system shall provide printout results containing candidates and/or issues in an alphanumeric format next to the vote totals.	Conduct a mock election and cast multiple votes. Once the voting is closed, print out results of the election using the supervisor functions.	Supervisor must close election and select the option to print votes cast. The printout presents the votes cast in a summary format.
3.39	The system shall allow for extraction of data from memory devices to a central host.	Close the election and transfer results to tally software (WinEDS).	Results transferred to WinEDS software with no problems.
3.40	The Tally software shall not allow the double counting of votes from a precinct or AVC Edge.	Upload election results from an AVC Edge voting machine to the tally software. Upload them a second time.	The software displays an error message when trying to upload the results twice from the same Card and does not allow the results to be uploaded.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.41	The Tally software shall not allow modification of the vote count.	Try to modify the vote tally in the WinEDS software using a tool such as MS Excel or MS Access.	WinEDS uses an MS SQL Server 2000 database. The Database sever contained an ODBC connection to the SQL Server database. Using MS Access from the administrator account, we were able to connect to the election results database and modify the data from the election. When connecting to the database with access, we enabled the "trusted connection" check box. We were also able to open the SQL Enterprise Manager without a password and modified the data.
3.42	The system shall provide for summary reports of votes cast on each voting device by extracting information from a memory device or a removable data storage device.	Conduct a mock election for two different AVC Edge (or memory devices) and verify a report can be created that list counts for each device.	Supervisor must close election by turning the switch to "Polls Closed" and select the option to print votes cast. Once all AVC Edge voting machines have closed all results are uploaded to WinEDS where reports are created. Reports can be created to show results for each AVC Edge.
3.43	The system shall provide for easily downloading results from balloting into the final tally of votes.	Conduct a mock election and have multiple voters cast ballots. Once the election is closed, the supervisor card must be used to select the option of transferring votes to WinEDS software for tallying and reporting.	Election results are easily downloaded to the Win EDS software through a PCMCIA reader attached to the computer where WinEDS software is installed.
3.44	The system shall accurately report all votes cast.	Set up a mock election and cast multiple votes. Verify all votes have been included in reports created by WinEDS.	All votes cast have been included in counts recorded by WinEDS software. All reports in WinEDS accurately reflect number of votes cast on AVC Edge.
3.45	The system shall provide a cumulative, canvass and precinct report of absentee voting, provisional ballot voting and Election Day voting as one total.	Verify election management software has the ability to handle provisional and absentee ballot voting.	Verified that functionality for recording absentee and provisional voting exists in the WinEDS software.

Continued on the next page

Requirements Tested & Test Results (continued)

No.	Requirement	Test Scenario	Test Results
3.46	The system shall provide a cumulative, canvass and precinct report of Election Day Voting as one total.	Conduct a mock election and close the election. Verify, through WINEDS, that all reports can be created by precinct. Also, verify provisional and absentee ballots can be included.	Printed the reports from the WinEDS software. Verified that provisional voting and absentee ballots were included.
3.47	The system shall not lose votes, corrupt media or have performance issues due to the presence of a magnetic field.	A magnet is placed on the LCD unit on the AVC Edge smart card reader when voting and PCMCIA slot when recording the votes.	There was no visible degradation on the display. During voting, the magnet did not have any effect on the smart card reader. The PCMCIA card did not get corrupted because of the magnetic field and no votes were lost.

Step 4: Controls Analysis

The Secretary of State has not been required to have a security plan in place for electronic voting systems in the past. As a result of HAVA, the requirement now exists.

Based on the findings of this report and the report developed by InfoSENTRY, the Secretary of State will develop a new security plan or modify the existing security plan to include risk mitigation strategies to minimize or eliminate the likelihood of threat.

Step 5: Threat Likelihood

In Step 5, the assessment team examined the threats identified in Step 2 against each potential vulnerability, and assigned a likelihood rating. The likelihood rating indicates the probability that a potential vulnerability may be exercised, taking into account the nature of the threat, motivation and capability of the threat-source (if human), and existence and effectiveness of current controls.

Each potential vulnerability was assigned a threat likelihood rating of High, Medium, or Low. The following table lists the potential vulnerabilities identified and their likelihood rating.

Potential Vulnerability Identified	Threat Likelihood Rating
Hacking	Medium
System intrusion, break-ins -Physical	Medium
Unauthorized system access- Physical	Medium
Fraudulent act	Low
Information bribery	Low
Spoofing	Low
System intrusion	Medium
Bomb/Terrorism	Low
Information warfare	Low
System attack	High
System penetration	High
System tampering	High
Economic exploitation	Low
Information theft	Medium
Intrusion on personal privacy	Low
Unauthorized system access (access to classified, proprietary, and/or technology-related information)	Medium
Unauthorized system access	Medium
System sabotage	High
System bugs	Low
Malicious code	Low
Fraud and theft	Low
Input of falsified, corrupted data	Low
Interception	Low

Step 6: Impact Analysis

In Step 6, the assessment team determined the adverse impact(s) that would likely occur if a threat-source were able to successfully exploit a vulnerability or weakness. The team followed the process below to determine the adverse impact resulting from a successful exploitation of a vulnerability:

- Determined the criticality of the electronic voting system and data to accomplishing the SOS' mission.
- Determined the probable adverse impact of a successful exploitation of a vulnerability.
- Determined the adverse impact of a security event in regard to loss or degradation of the system's integrity, availability, and confidentiality.
- Assigned a rating of High, Medium, or Low to each vulnerability to indicate the magnitude of impact resulting from a successful exploitation of the vulnerability.

The following table shows the magnitude of impact rating that was assigned to each potential vulnerability.

Potential Vulnerability Identified	Magnitude of Impact Rating
Code Review	
Data Integrity: In case of damage to the results cartridge, the election data can be retrieved from the internal memory of the AVC Edge unit. A consolidation card needs to be created from WinEDS, which is used to read the data from the AVC Edge. Current version of DREs do not verify the headers in the consolidation card to make sure it is for the same election.	High
Encryption: Ballot definitions, cast ballot records and audit log information are not encrypted. Encryption keys are not used for the PCMCIA card.	Low
Platform Review	
The AVC Edge enters supervisor mode without entry of any password or other security measures. Any voter could place the AVC Edge in supervisor mode in a few seconds.	High
We were able to read and modify portions of the Ballot Definition binary files on the PCMCIA card, but the system read the changed files as bad and would not load them onto the system.	Low

Continued on the next page

Step 6: Impact Analysis (continued)

Potential Vulnerability Identified	Magnitude of Impact Rating
An election can be closed on the AVC Edge by turning a switch on the back of the unit from the open position to the closed position. There is no password or confirmation entry requested. This switch can have a wire seal for protection. As an option, this switch can be ordered as a keyed switch.	Medium
The PCMCIA cards are loaded behind a plastic door that can be sealed with a wire seal. Anyone tampering with the cards would need to break the seal.	Low
The storage case does not have provisions for locks or seals. Only the internal seals attached to the PCMCIA case would provide evidence of tampering while the system was in storage or transported to an election.	Medium
Physical Testing	
PCMCIA card is easy to remove if compartment is not locked.	Low
The “close polls” switch can be accessed if it is not locked.	High
The Power OFF switch does not have a lock to secure it.	Low
The supervisor screen is not password-protected.	High
Risk of battery backups not connected properly.	Low
PCMCIA in transit to the Election Central counting location could be corrupted. This could result in lost votes since the votes are stored on the PCMCIA card.	Low

Step 7: Determine Risks

The purpose of Step 7 is to assess the level of risk to the electronic voting system. In this step, the assessment team identified the risk(s), if any, arising out of each test scenario. After identifying the risks, the team assigned a risk rating for each vulnerability by combining the results of the Impact Analysis established in Step 6 with the Likelihood of Threat established in Step 5. The combination of the impact analysis and the threat likelihood versus the security controls in place were applied to a risk-level matrix to determine the resultant risk-level.

Risks Identified

The assessment team identified the following vulnerabilities of the AVC Edge voting system. For each vulnerability identified, the table lists the relevant requirement tested, test scenario, and test results which identified the vulnerability.

No.	Test Scenario	Test Result	Risk Identified
Code Review			
1.01	Perform visual review of source files. Function names will be checked for proper case formatting of concatenated words. Names of functions should clearly describe its purpose.	Upon review of the code, it is noted that proper case formatting is used for function names and the names describe the purpose of the function.	None.
1.02	Perform visual review of source files. Modules should contain a consistent format and location for module components. Modules should begin with comments describing the modules contents. Location of methods and variables with associated comments should be consistent throughout.	Modules use a consistent format for comments and location of variables and methods. An exception is in the WinEDS 2.6 code, where comments were found to be limited to code blocks only.	None.
1.03	Perform visual review of source code. Modules should use a clear methodology of construction. Files will be reviewed to see if a coding industry standard is used in the naming of modules, functions, variables and constants.	Code follows an "industry" standard methodology in naming of modules, functions, variables and constants.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.04	Perform visual review of source code. Function and variable names should be "self documenting" as well as contain properly typed and sized attributes, and return types.	The function and variable names are self-describing and proper attribute and return types are used in the code.	None.
1.05	Perform visual review of source code for implementation of error handling code. All methods should contain error-handling logic. Systems should remain stable in the event of an error. When an error occurs, sufficient information regarding the state of the system and system parameters should be recorded for future debugging.	Upon review of the code, it is noted that proper error-handling procedures are implemented and appropriate messages/beeps are returned in the event of an error. The audit trail logs the important events in the results cartridge and the internal memory of the AVC Edge AVC Edge.	None.
1.06	Perform visual review of source code. Comments will be reviewed for simple descriptive content. Comments should appear at the beginning of each module, function. All module level variables, constants, and structures should be commented as well. Function parameters and return values should describe appropriate values. Comments should also appear in methods to help clarify complex code and logic behind expressions.	Upon review of the code, modules have comments at the beginning and comments are available for variables, constants, structures and complex logic. An exception is the WinEDS 2.6 code, which does not have comments at the beginning of each module. This application utilizes the PFC and these modules have header comments as originally provided by Sybase. The only comments found are for logical blocks of code.	None.
1.07	Perform visual review of source code. Comments should have a common format with standard fields for information. Some standard fields should be a description, parameters, return types, a change log.	A common format for comments is followed, with the following standard fields: description, parameters, return types and change log. An exception is the WinEDS 2.6 code, which does not have comments at the beginning of each module. This application utilizes the PFC and these modules have header comments as originally provided by Sybase. The only comments found are for logical blocks of code.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.08	Perform visual review of source code. Modules should have a standard comment identifier at the beginning of each module. Module comments should contain the name and description of the module, a copyright notice, and a change log.	Upon review of code, module comments contain name, a brief description of the module purpose, copyright notice and a detailed change log. An exception is the WinEDS 2.6 code, which does not have comments at the beginning of each module. This application utilizes the PFC and these modules have header comments as originally provided by Sybase.	WinEDS V2.6 source code does not contain sufficient comments in many modules to clearly convey the function of the modules. There is a risk that in future modifications to the WinEDS source code, it will be difficult to evaluate whether unauthorized functionality was included in the code changes and as a result the election process may be disrupted.
1.09	Perform visual review of the source code. Modules will be reviewed for their functional content. The variables and functions should be closely related and work directly to perform a clear task.	Code is available in the modules perform the specified tasks and unused variables/code was not found.	None.
1.10	The source code will be visually reviewed to verify if the code has been properly modularized. Modules should be an appropriate length and encapsulate related functionality.	Several modules with appropriate lengths have been created in the project.	None.
1.11	The source code will be visually reviewed for the use of simple and clear logical structures. There should be the use of constants (consts) and data structures (structs) to improve code readability and reliability.	Constants and data structures are used consistently in the system to improve readability and reliability.	None.
1.12	The source code will be visually reviewed to verify if the code has been properly modularized. Modules should encapsulate related functionality into logical groupings with clear interfaces. Interfaces should be well defined as to their use.	Upon review, it is noted that the code is properly modularized and the module size is managed correctly by implementing necessary functionality only.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.13	The source code will be visually reviewed to verify implementation of classes and proper modularization of the source files.	Most of the AVC Edge software is written in C. Since C does not implement classes, they have not been used. But proper modularization of code is done.	None.
1.14	The source code will be visually reviewed. The name and description of the class should be simple and clear. The task performed by the function should be easy to understand, simple to define, and atomic.	As noted above, the code has many modules and each implements a specific functionality. The module size makes the code readable and easy to understand.	None.
1.15	The source code will be visually reviewed to find any use of third party products. The makers and the versions of any found third party applications will be noted.	The following third party softwares are used in AVC Edge system: Phoenix BIOS, Metagraphics graphics functions, Menuet windowing system, Flash File System for ATA style PCMCIA flash ROM and CompactFlash.	None.
1.16	If the source is available for any used third party products, the source will be reviewed for client modifications. Third party source code should only contain the necessary functionality with unused areas removed or disabled. If the source is not available then further study will be required.	A specific boot code for the AVC Edge start up is used in the firmware. On review, it is noted that the third party software only provides specific functionality needed for AVC Edge system to function. Firmware updates are done using specially configured cartridge and a password to validate the cryptographic signatures on the files to be updated.	None.
1.17	The data model and database source code will be reviewed for existence of proper keys and normalization.	No database is used in the AVC Edge AVC Edge. Data files are stored in the results cartridge and resident memory of AVC Edge in proprietary format.	None.
1.18	The source code will be visually reviewed for user access levels and roles implemented as part of security in SQL Server 2000.	Not applicable to the design of AVC Edge.	None.
1.19	Source code will be reviewed and tested in order to check for CRC/Checksum techniques in verifying the correctness of data that is stored in memory. Can the software identify data that has been improperly modified?	CRC 16 algorithm has been implemented in the code to check for the correctness of the ballot image. Multiple read–write operations are implemented to make sure the data has not changed. This is done between each vote and power up.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.20	The source code will be reviewed to make sure that an algorithm is implemented to make sure voter records are stored in random order. The vote records should not have time stamp associated with it.	The vote records are stored in a random order in the results cartridge. A pseudo-random number generator (a 32-bit maximal length random sequence is seeded by the seconds portion of the internal clock) is implemented in the code.	None.
1.21	The source code will be reviewed to verify the system is secure and allows each voter to only vote once.	The smart cards used by voters are kept valid for a certain timeframe. Logic is implemented to de-activate the card by putting random data once it is used to enter a vote. Using the same card (without activation) gives a visual error message.	None.
1.22	The source code will be reviewed to verify there is a means by which votes can be recovered incase of a system disaster.	Recorded Votes and audit logs are stored in redundant memories (the internal memory in the AVC Edge and the results cartridge). In case of data mismatch, a consolidation card can be created from WinEDS software and used to read results from the AVC Edge.	None.
1.23	The strength of encryption will be reviewed. The types of encryption will be reviewed to see if it is sufficient.	The type of encryption used is DES (Data Encryption Standard) signed with SHA-1 (Secure Hash Algorithm). The cryptographic key appears to be derived from the hard-coded seed 1024 (refer to EEPROM_SZ in file Edgemap.h).	Sequoia has hard coded the encryption key seed number in their programs. There is a risk that an unauthorized person could break the encryption code and gain access to data on the DRE.
1.24	Ballot Definitions and Cast Vote Records should be protected and be verifiable they are correct. Encryption should be powerful enough to block access to stored data.	On examining the code, it is noted that the ballot definition and cast votes are not encrypted. At the time of closing the polls, cryptographic signatures are calculated and stored for each of the totals data files. These signatures are stored in both the audit trail and results cartridge.	The ballot definition and cast votes are not encrypted. There is a risk that an unauthorized person might access or modify the ballot definition and cast vote records.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.25	Various means of "voter identification" should be secure. The data on a voter authorization smart card should not be discernable.	The voter smart card is encrypted using DES signed with SHA-1.	None.
1.26	Encryption keys should be randomly generated every time and sufficiently long so that it is not easy to guess. The code will be reviewed to see if the keys are used in smart cards and PCMCIA cards.	Encrypted keys are not used in the results cartridge (PCMCIA card). The contents of the voter smart card are encrypted using DES and signed with SHA-1.	Data stored on the PCMCIA card is not encrypted. There is a risk that an unauthorized person might access or modify data stored on the PCMCIA card.
1.27	Transmission protocols will be checked for use on encryption. Data should never travel over a wire without protection. The contents of the transmission should be verifiable as to their contents and correctness. Any type of tampering should be identifiable if not impossible.	The AVC Edge system is not on a network. At the poll location, the results cartridge is inserted into the AVC Edge and the vote data and audit trail information is stored in the cartridge and internal memory of AVC edge unit. At close of polls, the results cartridges are physically transported to computer(s) at central location and are read by the WinEDS software to tally the results.	None.
1.28	Check the vote records on the AVC Edge, WinEDS software, and transfer medium to ensure that the records are encrypted.	The vote records and ballot information are not encrypted. Cryptographic signatures for each of the totals data files (ballot images, selection code summary totals and candidate summary totals) are computed and stored in the AVC Edge and results cartridge.	The ballot definition and cast votes are not encrypted. There is a risk that an unauthorized person could access or modify the cast vote records and ballot information.
1.29	Check the audit logs on the AVC Edge to ensure that they are encrypted.	Upon review of the code, it is noted that the audit log information in the AVC Edge or results cartridge are not encrypted.	Audit log information in the AVC Edge or results cartridge are not encrypted. There is a risk that an unauthorized person could view the audit log information.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
1.30	Perform code review to ensure that passwords used in all software are encrypted.	The AVC Edge does not require passwords during an election process. Passwords are required only while updating the firmware software. Based on the code, the technician password is in an encrypted database file. This file is not available for review.	None.
1.31	Perform code review to ensure that the system does not use hardcoded passwords.	On review of the code, hardcoded passwords were not found in the AVC Edge code.	None.
Platform Review			
2.01	Use the yellow button on the back of the AVC Edge to enter supervisor mode.	The AVC Edge enters supervisor mode without entry of any password or other security measures. Any voter could place the AVC Edge in supervisor mode in a few seconds.	The AVC Edge enters supervisor mode by pressing a button on the back of the terminal without entry of any password or other access controls. There is a risk that an unauthorized person might access supervisor mode on the AVC Edge and disrupt the polling process by executing supervisor functions.
2.02	Try to modify the Ballot Definition file on the PCMCIA result card before loading it on the AVC Edge.	We were able to read and modify portions of the Ballot Definition binary files on the PCMCIA card, but the system read the changed files as bad and would not load them onto the system.	None.
2.03	Install a program on a PCMCIA result card, insert it in the AVC Edge, and install and/or execute the unauthorized program.	The system did not load the unauthorized program from the PCMCIA card into the AVC Edge. It identified a bad file on the card and asked for the card to be removed. This test was run using an executable and a self-extracting executable file.	None.
2.04	Inspect the AVC Edge for network accessible ports.	The system contains an RS-232 serial port used for printing. The system also contains two PCMCIA slots. The card activator contains a 9 pin serial port.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
2.05	Try to access, modify, or disrupt the functioning of the AVC Edge software while connected to a network.	Attempts to manipulate the AVC Edge using a PCMCIA modem card attached to the PCMCIA slots resulted in an error message indicating the card was not recognized. No manipulation was possible.	None.
2.06	Try to bring the system down, lock up the operating system, change or erase log files, or any other form of Denial of Service (DoS), Distributed Denial of Service (DDos), or other result which benefits the attacker.	Attempts to disrupt the system failed. The system did not load the unauthorized program from the PCMCIA card into the AVC Edge AVC Edge.	None.
2.07	Try to gain admin rights or system rights using the switches and controls on the unit.	An election can be closed on the AVC Edge by turning a switch on the back of the unit from the open position to the closed position. This switch can have a wire seal for protection. As an option, this switch can be ordered as a keyed switch. Sequoia also provides an optional feature to prevent poll closure until a scheduled time. This option was not tested during the evaluation. There is no password or confirmation entry requested during closure. Supervisor rights can be gained by using the Activate button on the back of the AVC Edge once the polls are closed.	a) Polls are closed on the AVC Edge using a switch on the back of the DRE provided the preset election closing time has passed. No password is required to close the polls. A wire seal is available to cover the switch. Sequoia can provide a keyed switch for this function. There is a risk that an unauthorized person might close the polls on the AVC Edge. b) The AVC Edge enters supervisor mode by pressing a button on the back of the terminal after the polls are closed without entry of any password or other access controls. There is a risk that an unauthorized person might access the supervisor functions and use them to disrupt the election process.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
2.08	Try to cause a kernel panic, system failure, or indefinite wait state, or other operating system lock-up within the operating system or sub-system.	An election can be closed on the AVC Edge by turning a switch on the back of the unit from the open position to the closed position. This switch can have a wire seal for protection. As an option, this switch can be ordered as a keyed switch. Sequoia also provides an optional feature to prevent poll closure until a scheduled time. This option was not tested during the evaluation. There is no password or confirmation entry requested during closure. Supervisor rights can be gained by using the Activate button on the back of the AVC Edge once the polls are closed.	None.
2.09	Observe that functions are password protected, the minimum length of passwords, and that they can be changed.	Supervisor functions are not password protected.	Same as 2.07(b) – The AVC Edge enters supervisor mode by pressing a button on the back of the terminal without entry of any password or other access controls. There is a risk that an unauthorized person might access the supervisor functions and use them to disrupt the election process.
2.10	Try to create an attack on flash memory using files loaded on the PCMCIA result card.	The system would not read files from the PCMCIA card and read them as bad files on the card.	None.
2.11	Change the contents on a result media card and use the card. Determine if the system reports the card has been modified.	The system would not read files from the PCMCIA card and read them as bad files on the card.	None.
2.12	Try to modify protective counter.	There is no way to access the protective counter through menus, ports, the PCMCIA card, or other means.	None.
2.13	Observe the hardware and communication architecture to determine if such attacks are possible.	The AVC Edge is not on a LAN\WAN network and does not dial out over a phone line. Man-in-the-middle attacks are not possible.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
2.14	Try to gain access via an open TCP/UDP or serial or USB or other port.	There are no COM ports that will respond to an intruder. The printer serial port communicates one way.	None.
2.15	Try to introduce any type of malicious software (malware) into the system.	We were unable to load any type of malware into the AVC Edge. The system did not load the unauthorized program from the PCMCIA card into the AVC Edge.	None.
2.16	Inspect the hardware design documents and physical hardware.	The PCMCIA cards are loaded behind a plastic door that can be sealed with a wire seal. Anyone tampering with the cards would need to break the seal.	The PCMCIA card used on the AVC Edge is kept in a bay which can be protected by a wire seal. There is a risk that an unauthorized person might remove the PCMCIA card and disable the DRE.
2.17	Inspect the physical hardware for location of seals and locks.	The storage case does not have provisions for locks or seals. Only the internal seals attached to the PCMCIA case would provide evidence of tampering while the system was in storage or transported to an election.	The AVC Edge voting booth does not provide a means of locking the case. There is a risk that an unauthorized person could gain access to the AVC Edge during transportation to an election or while in storage.
2.18	Start voting on the AVC EDGE, and then disconnect batteries for 30 minutes to simulate a power outage. Resume power and start up the AVC EDGE, and check the voter information.	Once the AVC Edge batteries are drained to a critical level, the AVC Edge discontinues voting and shuts down. Once power is restored, voting can be resumed and no votes or audit information are lost.	None.
Physical Testing			
3.01	Check PCMCIA card to determine whether it can be removed easily and can be locked.	PCMCIA card is housed in a locked compartment and is not easy to remove when locked.	The PCMCIA card used on the AVC Edge is kept in a bay which can be protected by a wire seal. There is a risk that an unauthorized person might remove the PCMCIA card and disable the DRE.
3.02	Conduct logic and accuracy tests and verify system audit information is present.	Logic and accuracy tests were conducted before the election. System audit information is displayed on the resulting print out.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.03	Conduct logic and accuracy test and verify results are recorded in the on-board memory by printing the audit log.	Logic and accuracy tests were conducted before the election to verify system information was correct. Logic and accuracy test result were printed in the audit log.	None.
3.04	Conduct logic and accuracy testing before election is started. Print a zero tape before an election and a result tape after an election.	Logic and accuracy tests were conducted before the election to verify counters are working properly and the programming for each voting device is correct. A zero tape printout was created and verified that no votes were cast before the start of the election. After voting was closed, a result tape was printed.	None.
3.05	Create an instance where a known error will occur on the AVC Edge. For instance, enter a voter card after it has been de-activated.	AVC Edge displays a concise error message. This is standard throughout all error handling functions on the AVC Edge.	None.
3.06	Conduct a logic and accuracy test.	Logic and accuracy tests were conducted before the election to verify counters are working properly and the programming for each voting device is correct.	None.
3.07	Try to modify the Ballot Definition in the WinEDS software using a database viewer/program.	WinEDS uses an MS SQL Server 2000 database. The Database sever contained an ODBC connection to the SQL Server database. Using MS Access from the administrator account, we were able to connect to the election results database and modify the data from the election. When connecting to the database with access, we enabled the “trusted connection” check box. We were also able to open the SQL Enterprise Manager without a password and modified the data.	There is a risk that an unauthorized person with access to the administrator account on the EMS server might use any ODBC compliant product to access the Sequoia server and access or modify the database.
3.08	Create an election ballot definition file and transfer the file to the AVC EDGE. Open election and look at ballot.	The ballot is presented in a clear and unambiguous manner.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.09	Insert an authorized smart card into the AVC Edge voting machine and try to use it to vote multiple times.	Once a vote has been cast, the smart card used is deactivated. When trying to insert the deactivated smart card to vote again, the card is retained in the card reader.	None.
3.10	Insert a counterfeit smart card into the AVC Edge voting machine and try to use it to vote.	We were unable to manufacture a counterfeit voter card. Using an ACR80 Card Tool purchased on-line we were not able to read or write information onto the voter smart card and all attempts to manufacture a smart card were defeated.	We were unable to counterfeit a Voter smart card with the equipment we had available. This does not prove a working smart card cannot be counterfeited but does indicate it is not an easy task to accomplish. There is a risk that an unauthorized person might be able to create and use a counterfeit smart card and use it to cast extra ballots.
3.11	Create a counterfeit Voter Access smart card then attempt to use it so it is recognized and authenticated by the AVC Edge voting machine.	Unable to manufacture a counterfeit voter card. Voter card could not be read by the smart card reader.	None.
3.12	Access the supervisor screen and try to change the voting results during the election process.	The supervisor screen does not have the functions to change the vote results. Only the manual voting option and printing option for Zero tape are displayed if the polls are open.	None.
3.13	Access the supervisor screen and try to close the election.	The supervisor screen does not have the function to close the election. Turning the switch behind the AVC Edge to “Close polls” can close the election.	Polls are closed on the AVC Edge using a switch on the back of the DRE. No password is required to close the polls. A wire seal is available to cover the switch. Sequoia can provide a keyed switch for this function. There is a risk that an unauthorized person might close the polls on the AVC Edge.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.14	Access the supervisor screen and try to reset the AVC Edge.	The supervisor screen does not have the function to reset the AVC Edge after election process begins. But the Power OFF switch is accessible to the voter and can be turned off though this does not affect the voting process. When powered back ON, the AVC Edge starts up where the power was turned OFF. Once the polls are closed, the supervisor screen can reset the AVC Edge.	The AVC Edge Power OFF switch is accessible to the voter on the back of the DRE. Turning off power does not affect the voting process. When powered back ON, the AVC Edge starts up where the power was turned OFF. There is a risk that an unauthorized person might power off the AVC Edge during voting.
3.15	Access to supervisor screen using a PIN.	The AVC Edge allows access to the Supervisor screen without a PIN. The access is granted by a selection of special keystrokes.	The AVC Edge enters supervisor mode by pressing a button on the back of the terminal without entry of any password or other access controls. There is a risk that an unauthorized person might access supervisor mode on the AVC Edge and disrupt the polling process by executing supervisor functions.
3.16	Start voting on the AVC Edge, and then disconnect power for thirty minutes to simulate a power outage, and then resume power. Cast votes before, during, and after the disruption.	Power switch is easily accessible and when power is turned off, votes cast are still in system, but current voter must re-vote. The results of the previous votes are not lost and are stored in the AVC Edge and the PCMCIA card.	None.
3.17	Start voting on the AVC Edge, and then disconnect batteries for 30 minutes to simulate a power outage. Resume power and start up the AVC Edge, and check the voter information.	Once the AVC Edge batteries are drained to a critical level, the AVC Edge discontinues voting and shuts down. Once power is restored, voting can be resumed and no votes or audit information are lost.	None.
3.18	Try to modify the protective counter on the AVC Edge.	Supervisor functions will not allow the altering of counts on the AVC Edge voting machine. Counter is stored within the CPU on the AVC Edge. The number on the counter is printed out before the election and after the election as well.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.19	Modify the AVC Edge so that only core flash memory is available and see if the system will allow voting.	The AVC Edge will not operate unless removable flash memory is present in the existing slot. The AVC Edge displays an error message and does not allow any activities to take place until the card is inserted back into the AVC Edge.	None.
3.20	Try to access the supervisor screen.	The AVC Edge allows access to supervisor screens with the use of a combination of special keystrokes.	Same as 3.15 - The AVC Edge enters supervisor mode by pressing a button on the back of the terminal without entry of any password or other access controls. There is a risk that an unauthorized person might access supervisor mode on the AVC Edge and disrupt the polling process by executing supervisor functions.
3.21	Review audit log after completing successful vote test and ensure each step that used supervisor access is correctly logged.	Audit log is complete and accurate. It records all actions by the Supervisor on the AVC Edge.	None.
3.22	Print a copy of the audit log and verify all items are recorded.	Audit log was printed and all information listed in requirement was printed and verified.	None.
3.23	Print a copy of the audit log and verify all steps are recorded sequentially.	The audit log is generated in sequential order and each transaction within the audit log is time stamped.	None.
3.24	Review audit log after completing successful vote test and ensure each step that used supervisor access is correctly sequenced.	The Audit log records all the actions on the AVC Edge in the sequence in which the operations were performed.	None.
3.25	Review audit logs to verify any act will be recorded and logged with a timestamp.	All actions to the AVC Edge are recorded in the audit log with a time stamp. This includes opening and closing the polls, voting, inserting invalid voting cards, loss of power, and supervisor access.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.26	Try to access and modify the vote count on the PCMCIA before the vote count is loaded into the WinEDS software.	We were unable to alter vote counts on the PCMCIA card, which stores the data. After modifying the contents on the PCMCIA card, the WinEDS software doesn't recognize the PCMCIA card with the results.	The AVC Edge uses a PCMCIA card for transporting election results. This card can be read and written to using an ordinary Windows PC. We were unable to alter vote counts on the PCMCIA card. After modifying the contents on the PCMCIA card, the WinEDS software doesn't recognize the PCMCIA card with the results. There is a risk that an unauthorized person might corrupt the PCMCIA card in transit to the Election Central counting location.
3.27	Try to access the information needed to reconstruct a voter's exact voting record.	The Audit reports and the Summary reports from the AVC Edge cannot recreate the voters exact voting record. The supervisor screen does not have the function to view the exact voting records of each voter. The system will provide for provisional voting by creating a sequence to list provisional voter records.	None.
3.28	Verify vote cannot be altered once the ballot has been cast.	User cannot alter vote ballots cast. There is no supervisor function to allow for the votes cast to be altered.	None.
3.29	When the vote is being cast, others should not be allowed to view the voter's selection of preferences.	There are no supervisor functions to allow the view of a voter's selection. The supervisor must close the election to print reports. Curtains protect the voting booth.	None.
3.30	Verify reports can only be executed after the polls have been closed.	Reports can only be created when polls are closed. The Print option is enabled once the switch is turned to "Close Polls".	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.31	Conduct a mock election and try to trace votes to a voter.	The system does not allow any access to identify the Voter. The supervisor screen does not have this capability. After closing polls, the screen displays to print the summary report but does not provide the means to identify a voter with his/her ballot. Provisional voting is handled differently. Voter records can be re-constructed to verify if the vote cast is allowed or not allowed.	None.
3.32	Vote for all issues and/or candidates and before casting the ballot, verify a summary of all votes is presented.	A summary of all votes for each race for the particular user is displayed before we can cast the ballot. Corrections to any race can be made at this point.	None.
3.33	Try to modify the operating system on the AVC Edge by loading a new operating system off the PCMCIA card.	Attempted to load a counterfeit program using the PCMCIA card. The Program loaded into PCMCIA card was not recognized and was not loaded into the AVC Edge.	None.
3.34	As a Supervisor, print reports before closing the election.	Until the switch is turned to “Close Polls” the AVC Edge doesn’t give the option to print summary reports. The supervisor screen also does not have the Summary screen report option prior to closing the polls.	None.
3.35	Print out reports after election has been closed and verify no inaccuracies exist.	Printed election reports after the close of the election and verified no results were lost during this function.	None.
3.36	Close the election and print out a copy of the audit log and review all transactions.	All transactions are captured on the audit logs including specific information about the AVC Edge, definition of the election, and all actions occurring on the AVC Edge during the election. All items identified in this requirement are present.	None.
3.37	Complete and close an election and print out a copy of the audit log from a specific AVC EDGE.	An audit log is printed out using a specific supervisor function. The audit log produces a report that is a paper trail to guard against fraud.	None.

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.38	Conduct a mock election and cast multiple votes. Once the voting is closed, print out results of the election using the supervisor functions.	Supervisor must close election and select the option to print votes cast. The printout presents the votes cast in a summary format.	None.
3.39	Close the election and transfer results to tally software (WINEDS).	Results transferred to Win EDS software with no problems.	None.
3.40	Upload election results from an AVC Edge voting machine to the tally software. Upload them a second time.	The software displays an error message when trying to upload the results twice from the same Card and does not allow the results to be uploaded.	None.
3.41	Try to modify the vote tally in the WinEDS software using a tool such as MS Excel or MS Access.	WinEDS uses an MS SQL Server 2000 database. The Database sever contained an ODBC connection to the SQL Server database. Using MS Access from the administrator account, we were able to connect to the election results database and modify the data from the election. When connecting to the database with access, we enabled the "trusted connection" check box. We were also able to open the SQL Enterprise Manager without a password and modified the data.	There is a risk that an unauthorized person with access to the administrator account on the EMS server might use any ODBC compliant product to access the Sequoia server and access or modify the database.
3.42	Conduct a mock election for two different AVC Edge (or memory devices) and verify a report can be created that list counts for each device.	Supervisor must close election by turning the switch to "Polls Closed" and select the option to print votes cast. Once all AVC Edge voting machines have closed all results are uploaded to WinEDS where reports are created. Reports can be created to show results for each AVC Edge.	None.
3.43	Conduct a mock election and have multiple voters cast ballots. Once the election is closed, the supervisor card must be used to select the option of transferring votes to WinEDS software for tallying and reporting.	Election results are easily downloaded to the Win EDS software through a PCMCIA reader attached to the computer where WinEDS software is installed.	None.

Continued on the next page

Risks Identified (continued)

No.	Test Scenario	Test Result	Risk Identified
3.44	Set up a mock election and cast multiple votes. Verify all votes have been included in reports created by WinEDS.	All votes cast have been included in counts recorded by WinEDS software. All reports in WinEDS accurately reflect number of votes cast on AVC Edge.	None.
3.45	Verify election management software has the ability to handle provisional and absentee ballot voting.	Verified that functionality for recording absentee and provisional voting exists in the WinEDS software.	None.
3.46	Conduct a mock election and close the election. Verify, through WinEDS, that all reports can be created by precinct. Also, verify provisional and absentee ballots can be included.	Printed the reports from the WinEDS software. Verified that provisional voting and absentee ballots were included.	None.
3.47	A magnet is placed on the LCD unit on the AVC Edge smart card reader when voting and PCMCIA slot when recording the votes.	There was no visible degradation on the display. During voting, the magnet did not have any effect on the smart card reader. The PCMCIA card did not get corrupted because of the magnetic field and no votes were lost.	None.

Risk Levels of Identified Risks

Each Threat-Source/Vulnerability was assigned a rating of High, Medium, or Low to represent the degree or level of risk to which the electronic voting system might be exposed if a given vulnerability were exercised. Following is a description of the High, Medium, and Low Ratings.

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, it must determined whether corrective actions are still required or whether the risk can be accepted.

The following table shows the rating assigned to each identified risk.

No.	Risk Identified	Risk Likelihood	Impact Rating	Risk Level
Code Review				
1.08	WinEDS V2.6 source code does not contain sufficient comments in many modules to clearly convey the function of the modules. There is a risk that in future modifications to the WinEDS source code, it will be difficult to evaluate whether unauthorized functionality was included in the code changes and as a result the election process may be disrupted.	Low	High	Low
1.23	Sequoia has hard coded the encryption key seed number in their programs. There is a risk that an unauthorized person could break the encryption code and gain access to data on the DRE.	Low	Low	Low
1.24	The ballot definition and cast votes are not encrypted. There is a risk that an unauthorized person might access or modify the ballot definition and cast vote records.	Low	Medium	Low
1.26	Data stored on the PCMCIA card is not encrypted. There is a risk that an unauthorized person might access or modify data stored on the PCMCIA card.	Low	Medium	Low
1.28	The ballot definition and cast votes are not encrypted. There is a risk that an unauthorized person could access or modify the cast vote records and ballot information.	Low	Medium	Low
1.29	Audit log information in the AVC Edge or results cartridge are not encrypted. There is a risk that an unauthorized person could view the audit log information.	Low	Low	Low

Continued on the next page

Risk Levels of Identified Risks (continued)

No.	Risk Identified	Risk Likelihood	Impact Rating	Risk Level
Platform Review				
2.01	The AVC Edge enters supervisor mode by pressing a button on the back of the terminal without entry of any password or other access controls. There is a risk that an unauthorized person might access supervisor mode on the AVC Edge and disrupt the polling process by executing supervisor functions.	High	High	High
2.07(a)	Polls are closed on the AVC Edge using a switch on the back of the DRE provided the preset election closing time has passed. No password is required to close the polls. A wire seal is available to cover the switch. Sequoia can provide a keyed switch for this function. There is a risk that an unauthorized person might close the polls on the AVC Edge.	High	High	High
2.07(b) 2.09	The AVC Edge enters supervisor mode by pressing a button on the back of the terminal after the polls are closed without entry of any password or other access controls. There is a risk that an unauthorized person might access the supervisor functions and use them to disrupt the election process.	High	High	High
2.16	The PCMCIA card used on the AVC Edge is kept in a bay which can be protected by a wire seal. There is a risk that an unauthorized person might remove the PCMCIA card and disable the DRE.	Medium	High	Medium
2.17	The AVC Edge voting booth does not provide a means of locking the case. There is a risk that an unauthorized person could gain access to the AVC Edge during transportation to an election or while in storage.	High	Medium	Medium
Physical Testing				
3.01	The PCMCIA card used on the AVC Edge is kept in a bay which can be protected by a wire seal. There is a risk that an unauthorized person might remove the PCMCIA card and disable the DRE.	Medium	High	Medium
3.07	There is a risk that an unauthorized person with access to the administrator account on the EMS server might use any ODBC compliant product to access the Sequoia server and access or modify the database.	Low	High	Low
3.10	There is a risk that an unauthorized person might be able to create a counterfeit smart card and use it to cast extra ballots.	Low	Medium	Medium

Continued on the next page

Risk Levels of Identified Risks (continued)

No.	Risk Identified	Risk Likelihood	Impact Rating	Risk Level
3.13	Polls are closed on the AVC Edge using a switch on the back of the DRE. No password is required to close the polls. A wire seal is available to cover the switch. Sequoia can provide a keyed switch for this function. There is a risk that an unauthorized person might close the polls on the AVC Edge.	High	High	High
3.14	The AVC Edge Power OFF switch is accessible to the voter on the back of the DRE. Turning off power does not affect the voting process. When powered back ON, the AVC Edge starts up where the power was turned OFF. There is a risk that an unauthorized person might power off the AVC Edge during voting.	High	Medium	Medium
3.15 3.20	The AVC Edge enters supervisor mode by pressing a button on the back of the terminal without entry of any password or other access controls. There is a risk that an unauthorized person might access supervisor mode on the AVC Edge and disrupt the polling process by executing supervisor functions.	High	High	High
3.26	The AVC Edge uses a PCMCIA card for transporting election results. This card can be read and written to using an ordinary Windows PC. We were unable to alter vote counts on the PCMCIA card. After modifying the contents on the PCMCIA card, the WinEDS software doesn't recognize the PCMCIA card with the results. There is a risk that an unauthorized person might corrupt the PCMCIA card in transit to the Election Central counting location.	Medium	Medium	Medium
3.41	There is a risk that an unauthorized person with access to the administrator account on the EMS server might use any ODBC compliant product to access the Sequoia server and access or modify the database	Low	High	Low

Step 8: Risk Mitigation Strategies

In Step 8, the assessment team recommended solutions that are intended to mitigate or eliminate the risks identified in Step 7. The goal of the recommended risk mitigation strategies is to reduce the level of risk to the electronic voting system and its data to an acceptable level.

Recommended Risk Mitigation Strategies

The assessment team recommends the following mitigation strategies for the risks identified during this assessment.

Code Review

No.	Risk Identified	Recommended Mitigation Strategy
High Risk		
	N/A	
Medium Risk		
	N/A	
Low Risk		
1.08	WinEDS V2.6 source code does not contain sufficient comments in many modules to clearly convey the function of the modules. There is a risk that in future modifications to the WinEDS source code, it will be difficult to evaluate whether unauthorized functionality was included in the code changes and as a result the election process may be disrupted.	We recommend the Secretary of State require that Sequoia implement coding standards that include descriptive functional comments in all modules of WinEDS.
1.23	Sequoia has hard coded the encryption key seed number in their programs. There is a risk that an unauthorized person could break the encryption code and gain access to data on the DRE.	We recommend the Secretary of State require that Sequoia implement code changes to correct hard-coded seed to encryption key generation.
1.24	The ballot definition and cast votes are not encrypted. There is a risk that an unauthorized person might access or modify the ballot definition and cast vote records.	We recommend the Secretary of State require that Sequoia incorporate strong encryption to protect ballot definition and cast vote records.

Continued on the next page

Recommended Risk Mitigation Strategies (continued)

No.	Risk Identified	Recommended Mitigation Strategy
Low Risk (continued)		
1.26	Data stored on the PCMCIA card is not encrypted. There is a risk that an unauthorized person might access or modify data stored on the PCMCIA card.	We recommend the Secretary of State require that Sequoia incorporate strong encryption to protect data on the PCMCIA cards.
1.28	The ballot definition and cast votes are not encrypted. There is a risk that an unauthorized person could access or modify the cast vote records and ballot information.	We recommend the Secretary of State require that Sequoia incorporate strong encryption to protect data.
1.29	Audit log information in the AVC Edge or results cartridge is not encrypted. There is a risk that an unauthorized person could view the audit log information.	We recommend the Secretary of State require that Sequoia incorporate strong encryption to protect data.

Platform Review

No.	Risk Identified	Recommended Mitigation Strategy
High Risk		
2.01	The AVC Edge enters supervisor mode by pressing a button on the back of the terminal without entry of any password or other access controls. There is a risk that an unauthorized person might access supervisor mode on the AVC Edge and disrupt the polling process by executing supervisor functions.	We recommend the Secretary of State require that Sequoia provide password protection for supervisor functions.
2.07(a)	Polls are closed on the AVC Edge using a switch on the back of the DRE provided the preset election closing time has passed. No password is required to close the polls. A wire seal is available to cover the switch. Sequoia can provide a keyed switch for this function. There is a risk that an unauthorized person might close the polls on the AVC Edge.	We recommend the Secretary of State require that Sequoia provide keyed switches on all AVC Edge DREs deployed in Ohio. We also recommend the Secretary of State require that Sequoia provide password protection for closing the polls.
2.07(b) 2.09	The AVC Edge enters supervisor mode by pressing a button on the back of the terminal after the polls are closed without entry of any password or other access controls. There is a risk that an unauthorized person might access the supervisor functions and use them to disrupt the election process.	We recommend the Secretary of State require that Sequoia provide password protection for supervisor functions.

Continued on the next page

Recommended Risk Mitigation Strategies (continued)

No.	Risk Identified	Recommended Mitigation Strategy
Medium Risk		
2.16	The PCMCIA card used on the AVC Edge is kept in a bay which can be protected by a wire seal. There is a risk that an unauthorized person might remove the PCMCIA card and disable the DRE.	We recommend the Secretary of State require administrative procedures to ensure the PCMCIA card is protected from removal.
2.17	The AVC Edge voting booth does not provide a means of locking the case. There is a risk that an unauthorized person could gain access to the AVC Edge during transportation to an election or while in storage.	We recommend the Secretary of State require that Sequoia provide a means for attaching locks on all AVC Edge units.
Low Risk		
	N/A	

Physical Testing

No.	Risk Identified	Recommended Mitigation Strategy
High Risk		
3.13	Same as 2.07(a) under the Platform Review section above.	Same as 2.07(a) under the Platform Review section above.
3.15 3.20	Same as 2.01 under the Platform Review section above.	Same as 2.01 under the Platform Review section above.
Medium Risk		
3.01	Same as 2.16 under the Platform Review section above.	Same as 2.16 under the Platform Review section above.
3.10	We were unable to counterfeit a Voter smart card with the equipment we had available. This does not prove a working smart card cannot be counterfeited but does indicate it is not an easy task to accomplish. There is a risk that an unauthorized person might be able to create and use a counterfeit smart card to cast extra ballots.	We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk.

Continued on the next page

Recommended Risk Mitigation Strategies (continued)

Physical Testing (continued)

No.	Risk Identified	Recommended Mitigation Strategy
Medium Risk (continued)		
3.14	The AVC Edge Power OFF switch is accessible to the voter on the back of the DRE. Turning off power does not affect the voting process. When powered back ON, the AVC Edge starts up where the power was turned OFF. There is a risk that an unauthorized person might power off the AVC Edge during voting.	We recommend the Secretary of State require that Sequoia provide locks or seals on all DREs for the power switches.
3.26	The AVC Edge uses a PCMCIA card for transporting election results. This card can be read and written to using an ordinary Windows PC. We were unable to alter vote counts on the PCMCIA card. After modifying the contents on the PCMCIA card, the WinEDS software doesn't recognize the PCMCIA card with the results. There is a risk that an unauthorized person might corrupt the PCMCIA card in transit to the Election Central counting location.	We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk.
Low Risk		
3.07 3.41	There is a risk that an unauthorized person with access to the administrator account on the EMS server might use any ODBC compliant product to access the Sequoia server and access or modify the database.	We recommend the Secretary of State require that administrative policies and procedures be put into place to require use of proper Windows login security on the EMS server and to prevent unauthorized access, and not contain any additional software that would allow access to the EMS database.

Step 9: Document Results

In Step 9, the assessment team combined the results of Steps 1 through 8 to develop this report detailing the technical security assessment and its findings.

Conclusion

Compuware has conducted a study of the Sequoia AVC Edge voting system to identify specific security vulnerabilities that might be exploited during an election and to recommend actions to mitigate these vulnerabilities. The scope of this study has been limited to reviewing the technical implementation of the AVC Edge and reviewing each data stream into and from the AVC EDGE. It has not included a review of the policies, procedures, or work practices of either Sequoia or the Ohio Secretary of State.

During the course of our study, Compuware has identified several significant security issues, which left unmitigated would provide an opportunity for an attacker to disrupt the election process or throw the election results into question. These are documented above. Following careful consideration of each of these security issues, we have developed mitigation recommendations for the Secretary of State to implement which we believe will limit the likelihood of a successful attack on the election process. Provided each of these mitigation recommendations can be enacted, Compuware has concluded the Sequoia AVC Edge can be securely deployed by the Secretary of State.

Although all risks documented above must be dealt with appropriately, the most significant risk areas, which will require the most effort to mitigate, include:

Risk Identified	Recommended Mitigation Strategy
There is a risk that an unauthorized user could access unencrypted data stored on the PCMCIA card.	We recommend the Secretary of State require that Sequoia incorporate strong encryption to protect data.
The AVC Edge can be placed in supervisor mode using a button on the back of the DRE. Supervisor functions are not password protected. There is a risk that an unauthorized person can enter supervisor mode on the AVC Edge.	We recommend the Secretary of State require that Sequoia provide password protection for supervisor functions.
Polls are closed on the AVC Edge using a switch on the back of the DRE provided the preset election closing time has passed. No password is required to close the polls. A wire seal is available to cover the switch. Sequoia can provide a keyed switch for this function. There is a risk that an unauthorized person might close the polls on the AVC Edge.	We recommend the Secretary of State require that Sequoia provide keyed switches on all AVC Edge DREs deployed in Ohio. We also recommend the Secretary of State require that Sequoia provide password protection for closing the polls.
The AVC Edge voting booth case does not provide for locks. There is a risk that an unauthorized person could gain access to the AVC Edge during transportation to an election or while in storage.	We recommend the Secretary of State require that Sequoia install seals and locks on all DRE units.
There is a risk that the PCMCIA card can be removed if the compartment is not locked.	We recommend the Secretary of State require that Sequoia provide locks on all DREs.

Continued on the next page

Conclusion (continued)

Risk Identified	Recommended Mitigation Strategy
The power switch on the AVC Edge is not protected by a lock or seal. It is accessible on the back of the unit. There is a risk that an unauthorized person can power off the DRE during voting.	We recommend the Secretary of State require that Sequoia provide locks on all DREs for the power switches.
Sequoia uses a standard PCMCIA card for storing the ballot definitions and vote results. These cards can be easily placed in a laptop and altered. Due to protections in place, the altered card is unreadable by the DRE or election management software There is a risk that a PCMCIA in transit to the Election Central counting location could be corrupted.	We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk.

Election policies and procedures have long been used to ensure fair and accurate election results. The deployment of DRE technology will not lessen the need for well thought out and consistently enforced policies and procedures.

This page intentionally left blank.

ATTACHMENT A: Risk Assessment Methodology

Following is an explanation of the Risk Assessment methodology used by Compuware for this security assessment. The methodology used is in accordance with the National Institute of Standards and Technology (NIST) Nine Steps and is based upon the methodology documented in NIST SP 800-30, *Risk Management Guide for Information Technology Systems*.

The following information is based on NIST SP 800-30, which has been modified for use in this security assessment.

Overview

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an electronic voting system throughout its SDLC. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

Risk is a function of the *likelihood* of a given *threat-source's* exercising a particular potential *vulnerability*, and the resulting *impact* of that adverse event on the organization.

To determine the likelihood of a future adverse event, threats to an electronic voting system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT System in place. Impact refers to the magnitude of harm that could be caused by a threat's exercise of vulnerability. The level of impact is governed by the potential mission impacts and in turn produces a relative value for the IT assets and resources affected (e.g., the criticality and sensitivity of the electronic voting system components and data). The risk assessment methodology encompasses nine primary steps, which are described below.

Step 1. System Characterization (Section A.1)

Step 2. Threat Identification (Section A.2)

Step 3. Vulnerability Identification (Section A.3)

Step 4. Control Analysis (Section A.4)

Step 5. Likelihood Determination (Section A.5)

Step 6. Impact Analysis (Section A.6)

Step 7. Risk Determination (Section A.7)

Step 8. Control Recommendations (Section A.8)

Step 9. Results Documentation (Section A.9).

Steps 2, 3, 4, and 6 can be conducted in parallel after Step 1 has been completed.

Overview (continued)

Figure A-1 below depicts these steps.

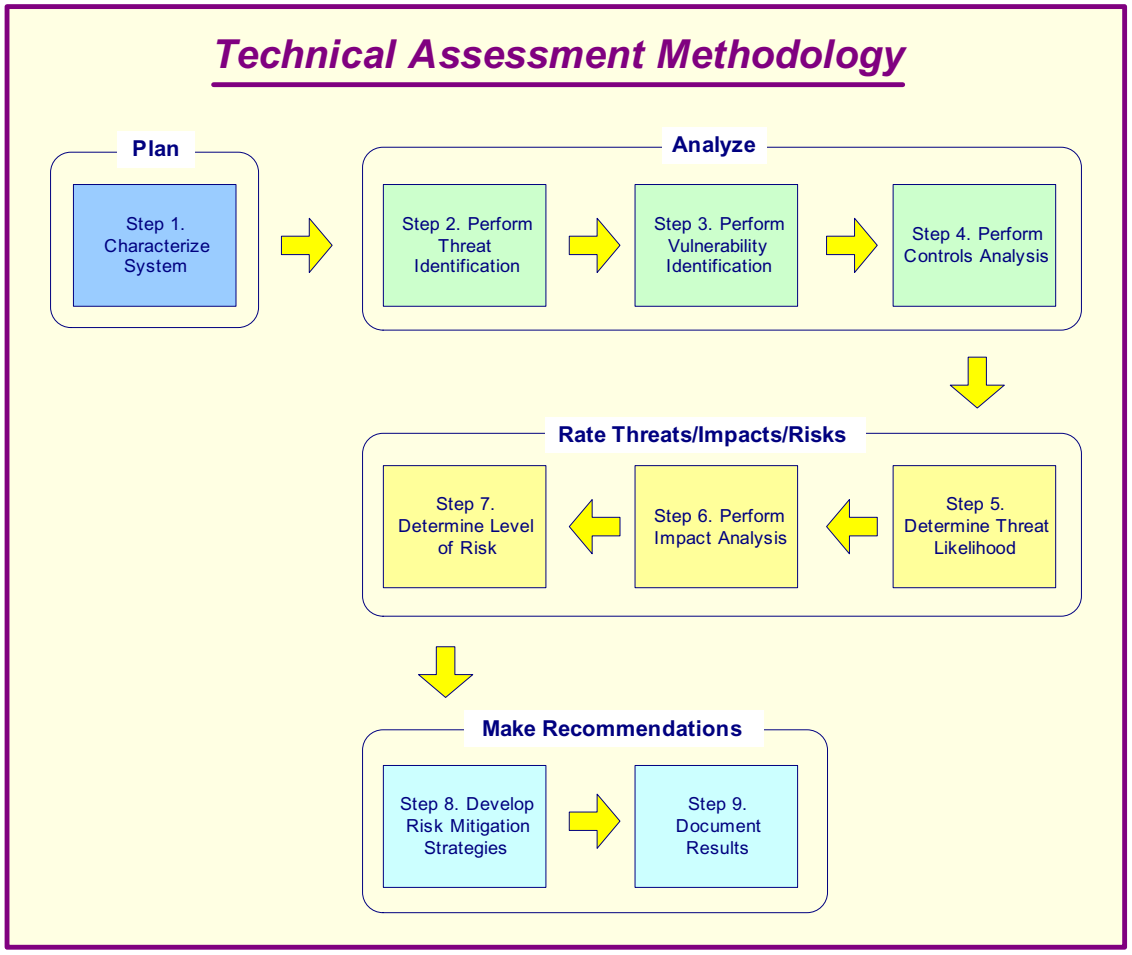

Figure A-1 – Technical Assessment Methodology

A.1 Step 1: System Characterization

In assessing risks for an electronic voting system, the first step is to define the scope of the effort. In this step, the boundaries of the electronic voting system are identified, along with the resources and the information that constitute the system. Characterizing an electronic voting system establishes the scope of the risk assessment effort, delineates the operational authorization (or accreditation) boundaries, and provides information (e.g., hardware, software, system connectivity, and responsible division or support personnel) essential to defining the risk.

Section A.1.1 describes the system-related information used to characterize an electronic voting system and its operational environment. Section A.1.2 suggests the information-gathering techniques that can be used to solicit information relevant to the electronic voting system processing environment.

The methodology described in this document can be applied to assessments of single or multiple, interrelated systems. In the latter case, it is important that the domain of interest and all interfaces and dependencies be well defined prior to applying the methodology.

A.1.1 System-Related Information

Identifying risk for an electronic voting system requires a keen understanding of the system's processing environment. The person or persons who conduct the risk assessment must therefore first collect system-related information, which is usually classified as follows:

- Hardware / Software / System interfaces (e.g., internal and external connectivity)
- Data and information
- Persons who support and use the electronic voting system
- System mission (e.g., the processes performed by the electronic voting system)
- System and data criticality (e.g., the system's value or importance to an organization)
- System and data sensitivity

Additional information related to the operational environmental of the electronic voting system and its data includes, but is not limited to, the following:

- The functional requirements of the electronic voting system
- Users of the system (e.g., system users who provide technical support to the electronic voting system; application users who use the electronic voting system to perform business functions)
- System security policies governing the electronic voting system (organizational policies, federal requirements, laws, industry practices)
- System security architecture
- Current network topology (e.g., network diagram)
- Information storage protection that safeguards system and data availability, integrity, and confidentiality
- Flow of information pertaining to the electronic voting system (e.g., system interfaces, system input and output flowchart)
- Technical controls used for the electronic voting system (e.g., built-in or add-on security product that supports identification and authentication, discretionary or mandatory access control, audit, residual information protection, encryption methods)

A.1.1 System-Related Information (continued)

Operational environment information (continued):

- Management controls used for the electronic voting system (e.g., rules of behavior, security planning)
- Operational controls used for the electronic voting system (e.g., personnel security, backup, contingency, and resumption and recovery operations; system maintenance; off-site storage; user account establishment and deletion procedures; controls for segregation of user functions, such as privileged user access versus standard user access)
- Physical security environment of the electronic voting system (e.g., facility security, data center policies)
- Environmental security implemented for the electronic voting system processing environment (e.g., controls for humidity, water, power, pollution, temperature, and chemicals).

For a system that is in the initiation or design phase, system information can be derived from the design or requirements document. For an electronic voting system under development, it is necessary to define key security rules and attributes planned for the future electronic voting system. System design documents and the system security plan can provide useful information about the security of an electronic voting system that is in development.

For an operational electronic voting system, data is collected about the electronic voting system in its production environment, including data on system configuration, connectivity, and documented and undocumented procedures and practices. Therefore, the system description can be based on the security provided by the underlying infrastructure or on future security plans for the electronic voting system.

A.1.2 Information-Gathering Techniques

Any, or a combination, of the following techniques can be used in gathering information relevant to the electronic voting system within its operational boundary:

Questionnaire

To collect relevant information, risk assessment personnel can develop a questionnaire concerning the management and operational controls planned or used for the electronic voting system. This questionnaire should be distributed to the applicable technical and no technical management personnel who are designing or supporting the electronic voting system. The questionnaire could also be used during on-site visits and interviews.

On-site Interviews

Interviews with electronic voting system support and management personnel can enable risk assessment personnel to collect useful information about the electronic voting system (e.g., how the system is operated and managed). On-site visits also allow risk

Assessment personnel to observe and gather information about the physical, environmental, and operational security of the electronic voting system. Appendix A contains sample interview questions asked during interviews with site personnel to achieve a better understanding of the operational characteristics of an organization. For systems still in the design phase, on-site visit would be face-to-face data gathering exercises and could provide the opportunity to evaluate the physical environment in which the electronic voting system will operate.

Document Review

Policy documents (e.g., legislative documentation, directives), system documentation (e.g., system user guide, system administrative manual, system design and requirement document, acquisition document), and security-related documentation (e.g., previous audit report, risk assessment report, system test results, system security plan, security policies) can provide good information about the security controls used by and planned for the electronic voting system. An organization's mission impact analysis or asset criticality assessment provides information regarding system and data criticality and sensitivity.

Use of Automated Scanning Tool

Proactive technical methods can be used to collect system information efficiently. For example, a network mapping tool can identify the services that run on a large group of hosts and provide a quick way of building individual profiles of the target electronic voting system(s).

Information gathering can be conducted throughout the risk assessment process, from Step 1 (System Characterization) through Step 9 (Results Documentation).

Output from Step 1

The outputs from Step 1 are: Characterization of the electronic voting system assessed, a good picture of the electronic voting system environment, and delineation of the system boundary.

A.2 Step 2: Threat Identification

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. Vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised. In determining the likelihood of a threat (Section A.5), one must consider threat-sources, potential vulnerabilities (Section A.3), and existing controls (Section A.4).

A.2.1 Threat-Source Identification

The goal of this step is to identify the potential threat-sources and compile a threat statement listing potential threat-sources that are applicable to the electronic voting system being evaluated.

- **Threat:** The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.
- **Threat-Source:** Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.

A threat-source is defined as any circumstance or event with the potential to cause harm to an electronic voting system. The common threat-sources can be natural, human, or environmental.

A.2.1 Threat-Source Identification (continued)

In assessing threat-sources, it is important to consider all potential threat-sources that could cause harm to an electronic voting system and its processing environment. For example, although the threat statement for an electronic voting system located in a desert may not include natural flood because of the low likelihood of such an event's occurring, environmental threats such as a bursting pipe can quickly flood a computer room and cause damage to an organization's IT assets and resources. Humans can be threat-sources through intentional acts, such as deliberate attacks by malicious persons or disgruntled employees, or unintentional acts, such as negligence and errors. A deliberate attack can be either (1) a malicious attempt to gain unauthorized access to an electronic voting system (e.g., via password guessing) in order to compromise system and data integrity, availability, or confidentiality or (2) a benign, but nonetheless purposeful, attempt to circumvent system security. One example of the latter type of deliberate attack is a programmer's writing a Trojan horse program to bypass system security in order to .get the job done.

A.2.2 Motivation and Threat Actions

Motivation and the resources for carrying out an attack make humans potentially dangerous threat-sources. The table below presents an overview of many of today's common human threats, their possible motivations, and the methods or threat actions by which they might carry out an attack. This information will be useful to organizations studying their human threat environments and customizing their human threat statements. In addition, reviews of the history of system break-ins; security violation reports; incident reports; and interviews with the system administrators, help desk personnel, and user community during information gathering will help identify human threat-sources that have the potential to harm an electronic voting system and its data and that may be a concern where vulnerability exists.

Common Threat-Sources

Natural Threats: Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.

Human Threats: Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, unauthorized access to confidential information).

Environmental Threats: Long-term power failure, pollution, chemicals, liquid leakage.

Continued on the next page

A.2.2 Motivation and Threat Actions (continued)

The following table describes the various human threats.

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Campaign and political entities	Competitive advantage Economic espionage Change outcome of election	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Continued on the next page

A.2.2 Motivation and Threat Actions (continued)

An estimate of the motivation, resources, and capabilities that may be required to carry out a successful attack should be developed after the potential threat-sources have been identified, in order to determine the likelihood of a threat's exercising system vulnerability, as described in Section 3.5.

The threat statement, or the list of potential threat-sources, should be tailored to the individual organization and its processing environment (e.g., end-user computing habits). In general, information on natural threats (e.g., floods, earthquakes, storms) should be readily available. Known threats have been identified by many government and private sector organizations. Intrusion detection tools also are becoming more prevalent, and government and industry organizations continually collect data on security events, thereby improving the ability to realistically assess threats. Sources of information include, but are not limited to, the following:

- Intelligence agencies (for example, the Federal Bureau of Investigation's National Infrastructure Protection Center)
- Federal Computer Incident Response Center (FedCIRC)
- Mass media, particularly Web-based resources such as SecurityFocus.com, SecurityWatch.com, SecurityPortal.com, and SANS.org.

Output from Step 2

The output from Step 2 is: A threat statement containing a list of threat-sources that could exploit electronic voting system vulnerabilities

A.3 Step 3: Vulnerability Identification

The analysis of the threat to an electronic voting system must include an analysis of the vulnerabilities associated with the system environment. The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources.

The following table presents examples of vulnerability/threat pairs.

Vulnerability	Threat-Source	Threat Action
Terminated employees. System identifiers (ID) are not removed from the system	Terminated employees	Dialing into the company's network and accessing company proprietary data
Company firewall allows inbound telnet, and guest ID is enabled on XYZ server	Unauthorized users (e.g., hackers, terminated employees, computer criminals, terrorists)	Using telnet to XYZ server and browsing system files with the guest ID
The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system	Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists)	Obtaining unauthorized access to sensitive system files based on known system vulnerabilities

Continued on the next page

A.3 Step 3: Vulnerability Identification (continued)

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Vulnerability	Threat-Source	Threat Action
Data center uses water sprinklers to suppress fire; tarpaulins to protect hardware and equipment from water damage are not in place	Fire, negligent persons	Water sprinklers being turned on in the data center

Recommended methods for identifying system vulnerabilities are the use of vulnerability sources, the performance of system security testing, and the development of a security requirements checklist.

It should be noted that the types of vulnerabilities that will exist, and the methodology needed to determine whether the vulnerabilities are present, will usually vary depending on the nature of the electronic voting system and the phase it is in, in the SDLC:

- If the electronic voting system has not yet been designed, the search for vulnerabilities should focus on the organization's security policies, planned security procedures, and system requirement definitions, and the vendors or developers security product analyses (e.g., white papers).
- If the electronic voting system is being implemented, the identification of vulnerabilities should be expanded to include more specific information, such as the planned security features described in the security design documentation and the results of system certification test and evaluation.
- If the electronic voting system is operational, the process of identifying vulnerabilities should include an analysis of the electronic voting system security features and the security controls, technical and procedural, used to protect the system.

Continued on the next page

A.3 Step 3: Vulnerability Identification (continued)

A.3.1 Vulnerability Sources

The technical and no technical vulnerabilities associated with an electronic voting system's processing environment can be identified via the information-gathering techniques described in Section 3.1.2. A review of other industry sources (e.g., vendor Web pages that identify system bugs and flaws) will be useful in preparing for the interviews and in developing effective questionnaires to identify vulnerabilities that may be applicable to specific electronic voting systems (e.g., a specific version of a specific operating system). The Internet is another source of information on known system vulnerabilities posted by vendors, along with hot fixes, service packs, patches, and other remedial measures that may be applied to eliminate or mitigate vulnerabilities. Documented vulnerability sources that should be considered in a thorough vulnerability analysis include, but are not limited to, the following:

- Previous risk assessment documentation of the electronic voting system assessed
- The electronic voting system's audit reports, system anomaly reports, security review reports, and system test and evaluation reports
- Vulnerability lists, such as the NIST I-CAT vulnerability database (http://icat.nist.gov)
- Security advisories, such as FedCIRC and the Department of Energy's Computer Incident Advisory Capability bulletins
- Vendor advisories
- Commercial computer incident/emergency response teams and post lists (e.g., SecurityFocus.com forum mailings)
- Information Assurance Vulnerability Alerts and bulletins for military systems
- System software security analyses.

A.3.2 System Security Testing

Proactive methods, employing system testing, can be used to identify system vulnerabilities efficiently, depending on the criticality of the electronic voting system and available resources (e.g., allocated funds, available technology, persons with the expertise to conduct the test). Test methods include.

- Automated vulnerability scanning tool
- Security test and evaluation (ST&E)
- Penetration testing

The automated vulnerability scanning tool is used to scan a group of hosts or a network for known vulnerable services (e.g., system allows anonymous File Transfer Protocol [FTP], send mail relaying). However, it should be noted that some of the potential vulnerabilities identified by the automated scanning tool may not represent real vulnerabilities in the context of the system environment. For example, some of these scanning tools rate potential vulnerabilities without considering the site's environment and requirements. Some of the vulnerabilities flagged by the automated scanning software may actually not be vulnerable for a particular site but may be configured that way because their environment requires it. Thus, this test method may produce false positives.

Continued on the next page

A.3 Step 3: Vulnerability Identification (continued)

ST&E is another technique that can be used in identifying electronic voting system vulnerabilities during the risk assessment process. It includes the development and execution of a test plan (e.g., test script, test procedures, and expected test results). The purpose of system security testing is to test the effectiveness of the security controls of an electronic voting system as they have been applied in an operational environment. The objective is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards.

Penetration testing can be used to complement the review of security controls and ensure that different facets of the electronic voting system are secured. Penetration testing, when employed in the risk assessment process, can be used to assess an electronic voting system's ability to withstand intentional attempts to circumvent system security. Its objective is to test the electronic voting system from the viewpoint of a threat-source and to identify potential failures in the electronic voting system protection schemes.

The results of these types of optional security testing will help identify a system's vulnerabilities.

A.3.3 Development of Security Requirements Checklist

During this step, the risk assessment personnel determine whether the security requirements stipulated for the electronic voting system and collected during system characterization are being met by existing or planned security controls. Typically, the system security requirements can be presented in table form, with each requirement accompanied by an explanation of how the system's design or implementation does or does not satisfy that security control requirement.

A security requirements checklist contains the basic security standards that can be used to systematically evaluate and identify the vulnerabilities of the assets (personnel, hardware, software, and information), non automated procedures, processes, and information transfers associated with a given electronic voting system in the following security areas:

- Management
- Operational
- Technical

Continued on the next page

A.3 Step 3: Vulnerability Identification (continued)

The following table lists security criteria suggested for use in identifying an electronic voting system's vulnerabilities in each security area.

Security Area	Security Criteria
Management Security	• Assignment of responsibilities • Continuity of support • Incident response capability • Periodic review of security controls • Personnel clearance and background investigations • Risk assessment • Security and technical training • Separation of duties • System authorization and reauthorization • System or application security plan
Operational Security	• Control of air-borne contaminants (smoke, dust, chemicals) • Controls to ensure the quality of the electrical power supply • Data media access and disposal • External data distribution and labeling • Facility protection (e.g., computer room, data center, office) • Humidity control • Temperature control • Workstations, laptops, and stand-alone personal computers
Technical Security	• Communications (e.g., dial-in, system interconnection, routers) • Cryptography • Discretionary access control • Identification and authentication • Intrusion detection • Object reuse • System audit

The outcome of this process is the security requirements checklist. Sources that can be used in compiling such a checklist include, but are not limited to, the following government regulatory and security directives and sources applicable to the electronic voting system processing environment:

- CSA of 1987 Federal Information
- Processing Standards Publications
- OMB November 2000 Circular A-130
- Privacy Act of 1974
- System security plan of the electronic voting system assessed
- The organization's security policies, guidelines, and standards
- Industry practices.

Continued on the next page

A.3 Step 3: Vulnerability Identification (continued)

The NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, provides an extensive questionnaire containing specific control objectives against which a system or group of interconnected systems can be tested and measured. The control objectives are abstracted directly from long-standing requirements found in statute, policy, and guidance on security and privacy.

The results of the checklist (or questionnaire) can be used as input for an evaluation of compliance and noncompliance. This process identifies system, process, and procedural weaknesses that represent potential vulnerabilities.

A.4 Step 4: Control Analysis

The goal of this step is to analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability.

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment (Step 5 below), the implementation of current or planned controls must be considered. For example, a vulnerability (e.g., system or procedural weakness) is not likely to be exercised or the likelihood is low if there is a low level of threat-source interest or capability or if there are effective security controls that can eliminate, or reduce the magnitude of, harm.

Sections A.4.1 through A.4.3, respectively, discuss control methods, control categories, and the control analysis technique.

A.4.1 Control Methods

Security controls encompass the use of technical and non technical methods. Technical controls are safeguards that are incorporated into computer hardware, software, or firmware (e.g., access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software). Non technical controls are management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security.

A.4.2 Control Categories

The control categories for both technical and non technical control methods can be further classified as either preventive or detective. These two subcategories are explained as follows:

Preventive controls inhibit attempts to violate security policy and include such controls as access control enforcement, encryption, and authentication.

Detective controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums.

Section 4.4 further explains these controls from the implementation standpoint. The implementation of such controls during the risk mitigation process is the direct result of the identification of deficiencies in current or planned controls during the risk assessment process (e.g., controls are not in place or controls are not properly implemented).

A.4.3 Control Analysis Technique

As discussed in Section A.3.3, development of a security requirements checklist or use of an available checklist will be helpful in analyzing controls in an efficient and systematic manner. The security requirements checklist can be used to validate security noncompliance as well as compliance. Therefore, it is essential to update such checklists to reflect changes in an organization's control environment (e.g., changes in security policies, methods, and requirements) to ensure the checklist's validity.

Output from Step 4

The output from Step 4 is: List of current or planned controls used for the electronic voting system to mitigate the likelihood of vulnerabilities being exercised and reduce the impact of such an adverse event.

A.5 Step 5: Likelihood Determination

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment; the following governing factors must be considered:

- Threat-source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls

The likelihood that a potential vulnerability could be exercised by a given threat-source can be described as high, medium, or low. The table below describes these three likelihood levels.

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 vulnerability from being exercised.

Output from Step 5

The output from Step 5 is: Likelihood rating (High, Medium, Low) for the potential vulnerability.

A.6 Step 6: Impact Analysis

The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of vulnerability. Before beginning the impact analysis, it is necessary to obtain the following necessary information as discussed in Section 3.1.1:

- System mission (e.g., the processes performed by the electronic voting system)
- System and data criticality (e.g., the system's value or importance to an organization)
- System and data sensitivity

This information can be obtained from existing organizational documentation, such as the mission impact analysis report or asset criticality assessment report. A mission impact analysis (also known as business impact analysis [BIA] for some organizations) prioritizes the impact levels associated with the compromise of an organization's information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets. An asset criticality assessment identifies and prioritizes the sensitive and critical organization information assets (e.g., hardware, software, systems, services, and related technology assets) that support the organization's critical missions.

If this documentation does not exist or such assessments for the organization's IT assets have not been performed, the system and data sensitivity can be determined based on the level of protection required to maintain the system and data's availability, integrity, and confidentiality. Regardless of the method used to determine how sensitive an electronic voting system and its data are, the system and information owners are the ones responsible for determining the impact level for their own system and information. Consequently, in analyzing impact, the appropriate approach is to interview the system and information owner(s).

Therefore, the adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: integrity, availability, and confidentiality. The following list provides a brief description of each security goal and the consequence (or impact) of its not being met:

Loss of Integrity: System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or electronic voting system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an electronic voting system.

Loss of Availability: If a mission-critical electronic voting system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users. Performance of their functions in supporting the organization's mission.

Loss of Confidentiality: System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

Continued on the next page

A.6 Step 6: Impact Analysis (continued)

Some tangible impacts can be measured quantitatively in lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other impacts (e.g., loss of public confidence, loss of credibility, damage to an organization's interest) cannot be measured in specific units but can be qualified or described in terms of high, medium, and low impacts. Because of the generic nature of this discussion, this guide designates and describes only the qualitative categories, high, medium, and low impact (see the table below).

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 an 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.

Quantitative versus Qualitative Assessment

In conducting the impact analysis, consideration should be given to the advantages and disadvantages of quantitative versus qualitative assessments. The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities. The disadvantage of the qualitative analysis is that it does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-benefit analysis of any recommended controls difficult.

The major advantage of a quantitative impact analysis is that it provides a measurement of the impacts. Magnitude, which can be used in the cost-benefit analysis of recommended controls. The disadvantage is that, depending on the numerical ranges used to express the measurement, the meaning of the quantitative impact analysis may be unclear, requiring the result to be interpreted in a qualitative manner. Additional factors often must be considered to determine the magnitude of impact. These may include, but are not limited to:

- An estimation of the frequency of the threat-source's exercise of the vulnerability over a specified time period (e.g., 1 year)
- An approximate cost for each occurrence of the threat-source's exercise of the vulnerability
- A weighted factor based on a subjective analysis of the relative impact of a specific threat's exercising a specific vulnerability.

Output from Step 6

The output from Step 6 is: Magnitude of impact rating (High, Medium, or Low).

A.7 Step 7: Risk Determination

The purpose of this step is to assess the level of risk to the electronic voting system. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of:

- The likelihood of a given threat-source's attempting to exercise a given vulnerability
- The magnitude of the impact should a threat-source successfully exercise the vulnerability
- The adequacy of planned or existing security controls for reducing or eliminating risk.

To measure risk, a risk scale and a risk-level matrix must be developed. Section A.7.1 presents a standard risk-level matrix; Section A.7.2 describes the resulting risk levels.

A.7.1 Risk-Level Matrix

The final determination of mission risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact. The table below shows how the overall risk ratings might be determined based on inputs from the threat likelihood and threat impact categories. The matrix below is a 3 x 3 matrix of threat likelihood (High, Medium, and Low) and threat impact (High, Medium, and Low). Depending on the site's requirements and the granularity of risk assessment desired, some sites may use a 4 x 4 or a 5 x 5 matrix. The latter can include Very Low /Very High threat likelihood and a Very Low/Very High threat impact to generate a Very Low/Very High risk level. A Very High risk level may require possible system shutdown or stopping of all electronic voting system integration and testing efforts.

The sample matrix in the table below shows how the overall risk levels of High, Medium, and Low are derived. The determination of these risk levels or ratings may be subjective. The rationale for this justification can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level.

For example:

- The probability assigned for each threat likelihood level is 1.0 for High, 0.5 for Medium, 0.1 for Low
- The value assigned for each impact level is 100 for High, 50 for Medium, and 10 for Low.

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	High 100 x 0.5 = 50
Low (0.1)	Low 10 x 0.1 = 1	Medium 50 x 0.1 = 5	High 100 x 0.1 = 10

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

A.7.2 Description of Risk Level

The table below describes the risk levels shown in the above matrix. This risk scale, with its ratings of High, Medium, and Low, represents the degree or level of risk to which an electronic voting system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk scale also presents actions that senior management, the mission owners, must take for each risk level.

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, it must determined whether corrective actions are still required or whether the risk can be accepted.

Output from Step 7

The output from Step 7 is: Risk level (High, Medium, Low).

A.8 Step 8: Control Recommendations

During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided. The goal of the recommended controls is to reduce the level of risk to the electronic voting system and its data to an acceptable level. The following factors should be 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

The control recommendations are the results of the risk assessment process and provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.

It should be noted that not all possible recommended controls can be implemented to reduce loss. To determine which ones are required and appropriate for a specific organization, a cost-benefit analysis, as discussed in Section 4.6, should be conducted for the proposed recommended controls, to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. In addition, the operational impact (e.g., effect on system performance) and feasibility (e.g., technical requirements, user acceptance) of introducing the recommended option should be evaluated carefully during the risk mitigation process.

Output from Step 8

The output from Step 8 is: Recommendation of control(s) and alternative solutions to mitigate risk.

A.9 Step 9: Results Documentation

Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results should be documented in an official report or briefing.

A risk assessment report is a management report that helps senior management, the mission owners, make decisions on policy, procedural, budget, and system operational and management changes. Unlike an audit or investigation report, which looks for wrongdoing, a risk assessment report should not be presented in an accusatory manner but as a systematic and analytical approach to assessing risk so that senior management will understand the risks and allocate resources to reduce and correct potential losses. For this reason, some people prefer to address the threat/vulnerability pairs as observations instead of findings in the risk assessment report.

Output from Step 9

The output from Step 9 is: A Risk Assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.

ATTACHMENT B: Glossary

Term	Meaning
ACL	Access Control Lists
ADA	Americans With Disabilities Act
ATA	Advanced Technology Attachment
BIOS	Basic Input/Output System
BOE	Board of Elections
BOSS	Ballot Origination Software System
C&A	Certification and Accreditation
CIO	Chief Information Officer
Context Diagram	Diagram that provides a graphical overview of the input/output connections between the DRE and external entities such as the BOE's and voters. The context diagram helps to define the scope of the voting system/process and becomes the top level of the analysis hierarchy.
COOP	Continuity of Operations
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
Cryptographic Analysis	Analysis of the strength and methods of data protection using encryption and Cyclic Redundancy Checks.
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DoS	Denial of Service
DOS	Disk Operating System
DR	Disaster Recovery
DRAM	Dynamic Random Access Memory
DRE	Direct Recording Electronic voting machine
EMS	Election Management System
ES&S	Electronic Systems and Software
Exploitation Analysis	Analysis of how and by what means an attacker, if able to discover any weak points in the system, can use weak areas to attack the integrity of a DRE.
FEC	Federal Election Commission
GSS	General Support System
GUI	Graphical User Interface
HAL	Hardware Abstraction Layer

Continued on the next page

Term	Meaning
HAVA	Help America Vote Act of 2002
IDE	Integrated Drive Electronics
IDS	Intrusion detection system
Impact Analysis	Analysis of the impacts that could occur if an attacker was able to use a DRE's weakness to affect an election.
IrDA	Infrared Data Association. IrDA ports enable the transfer of data from one device to another via infrared light waves instead of cables.
IT	Information Technology
ITA	Independent Testing Authority
JBC	Judge's Booth Controller
LAN	Local Area Network
LAT	Logic and Accuracy Testing
LCD	Liquid Crystal Display
M2B3	Multiple Mobile Ballot Box Bay
MB	Megabytes
MBB	Mobile Ballot Box
MFC	Microsoft Foundation Classes
MHz	Megahertz
MQX	MQX Real Time Operating System
NIST	National Institute of Standards and Technology
Overvote	To vote for more than the allotted number of candidates
OS	Operating System
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association. PCMCIA cards (or PC cards) are small, credit card-sized devices that were originally designed for adding additional memory to personal computers. There are now several types of these cards for various uses.
PEB	Personal Electronic Ballot
PFC	PowerBuilder Foundation Class
PIN	Personal Identification Number
POC	Point of Contact
Process Model	Diagram that displays the flow of data through the DRE; represents the next level down from the Context Diagram.
PVS	Precinct Voting System
QA	Quality Assurance

Continued on the next page

Term	Meaning
RA	Risk Assessment
Reconnaissance Analysis	Analysis for the purpose of gaining information on potential ways that an attacker may be able to gain access to a system.
RAM	Random Access Memory
ROM	Read Only Memory
RTOS	Real Time Operating System
SAIC	Science Applications International Corporation
Smart Card	A small electronic device about the size of a credit card that contains electronic memory, and possibly an embedded integrated circuit.
SOCC	State of Ohio Computer Center
SOS	Ohio Secretary of State
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UES	Unity Election System
Undervote	To vote for less than the allotted number of candidates
VPN	Virtual Private Network
VSB	Vestigial Side Band
WAN	Wide Area Network

This page intentionally left blank.

ATTACHMENT C: Documents Referenced

During this technical security assessment, Compuware reviewed all available documentation relating to the system, its setup, storage, operations and maintenance. Following is a list of the documents that were reviewed during this technical security assessment.

File Name if Electronic	Document Title or Description
Diebold	
Codeset files for AccuVote-TS R6, Firmware version 4.3.15	
Codeset files for Voter Card Encoder version 1.1.4	
Codeset files for Global Election Management System (GEMS) version 1.18.18	
Diebold.pdf	Diebold's response to State of Ohio Proposal for Statewide Voting System
GEMS_1.18_Users_Guide_Revision_6.0.pdf	GEMS 1.18 User's Guide, Revision 6.0, Diebold Election Systems
readme.htm	Diebold Election Systems Inc., GEMS 1.18.18 Release Notes, June 6, 2003
BS GEMS User Guide.zip.sda.exe	GEMS User's Guide
ES&S	
Codeset files for iVotronic version 7.4.5.0	
Codeset files for Unity Election System software version 2.2	
Codeset files for PEB	
Ohio State Final Document.pdf	Statewide Voting Systems for the State of Ohio, Part 1 – Administrative Documents and Technical Proposal, RFP Number SOS0428365
ES&S 45827.pdf	ITA Qualification Testing of the ES&S Model iVotronic DRE Precinct Counter, Firmware Release 7.4.5.0 (Wyle Laboratories Document No. 45827B-028)
ESS 45827-01 Rev. A.pdf	Wyle Test Report, Qualification Testing of the iVotronic DRE Precinct Counter (Revision A, Wyle Report No. 45827-01, Firmware Release 6.1.2, October 30, 2001)
Unity 2.2 readme.doc	Unity 2.2 Change Release Note
software Compilers-assemblers.doc	Unity 2.2 Compilers/Assemblers

Continued on the next page

File Name if Electronic	Document Title or Description
ES&S (continued)	
iVo Change Release 7.4.5.0.doc	iVotronic Change Release Summary, Version 7.4.4.0 – 7.4.5.0, July 19, 2002
Data Acquisition Manager Software Specs.doc	Data Acquisition Manager System Software Specification, Version 1.98 — April 2001
EDMSystem.doc	Election Data Manager System Software Specification, Version 5.7 Dec 2000
ESS BIM sft specs.doc	ES&S Image Manager System Software Specification, Version 6.0.1 May 2001
iVot Image Manager Software specs2.doc	Unity Ballot Image Manager, iVotronic, Software Specifications, Version 1.0 – April, 2002
Prog Mngr Software Specs.doc	Hardware Programming Manager System Software Specification, Version 3.53 — March 2001
UERMSystem.doc	Election Reporting Manager System Software Specification, Version 6.19 — August 2001
ivotronic maintenance 7.4.pdf	The iVotronic Voting System Maintenance Manual, Version 7.4 (Version Release 7.4, Hardware Version 1.0, July 25, 2002)
iVotronic 7.4 (bat.charger).pdf	The iVotronic Voting System Operator's Manual, Version 7.4, July 25, 2002
DAM 2_4__4_2(edit).doc	Unity Data Acquisition Manager User's Guide, Version 4.2 Remote, 2.4 Host (July 18, 2002)
Data Manager 7.1 users.doc	Unity Election Data Manager User's Guide, Version 7.1, (July 23, 2002)
ERM 6.3.0.doc	Unity Election Reporting Manager User's Guide, Version 6.3 (June 19, 2002)
HPM oper reformat mn 3.6.0.0.doc	Unity Hardware Programming Manager User's Guide, Version 3.6.0.0 (June 24, 2002)
iVotronic Image Manager 1-1.doc	Unity Ballot Image Manager, iVotronic Image Manager User's Guide, Version Release 1.1 (June 26, 2002)
Unity 2.2 System Limits(edit 2 CM).doc	Limitations of the Unity System 2.2 With iVotronic, M100, M150/550, M650
Hart InterCivic	
Codeset files for eSlate 3000 version 2.1	
Codeset files for Judge's Booth Controller (JBC) version 1.16	
Codeset files for BOSS Election Management Software version 2.9.04	

Continued on the next page

File Name if Electronic	Document Title or Description
Hart InterCivic (continued)	
Codeset files for TALLY software version 2.9.08	
Codeset files for SERVO software version 1.0.2	
(n/a)	SERVO Documentation System 2.1, SERVO Design Specification (Revision C, September 26, 2002)
(n/a)	System 2.1 Requirements BOSS 2.9, TALLY 2.9, PVS 1.16 (Version 0.02, June 3, 2002)
(n/a)	BOSS Documentation System 2.1, Data Model, BOSS Design Documentation (Revision H, May 28, 2002)
(n/a)	Tally Documentation System 2.1, Object Model, Tally Design Specification (Revision H, August 22, 2001)
MAXIMUS Combined.doc and appendix files	Maximus/Hart InterCivic's response to State of Ohio RFP Number SOS0428365
Sequoia	
Codeset files for AVC Edge version 4.1. D	
Codeset files for Card Activator version 4.2	
Codeset files for WinEDS Election Management Software version 2.6	
(various files)	WinEDS Reference Guide Version 2.6
Installation 2-6 Guide.pdf	WinEDS 2.6 Initial Installation Guide
Upgrade 2-6 Guide.pdf	WinEDS 2.6 Upgrade/Installation Guide
WinEDS 2-6 212 Installation Files List.doc	WinEDS 2.6 Build 212 Installed Files Listing
AVC Edge 4.1 Coding Standards.doc	AVC Edge Coding Standards Release 4.1
AVC Edge 4.1 Data Dictionary.doc	AVC Edge Data Dictionary For Release 4.1
AVC Edge 4.1 Functional Spec.doc	AVC Edge Functional Specification Release 4.1
AVC Edge 4.1 Penetration Analysis.doc	AVC Edge Penetration Analysis Release 4.1
AVC Edge 4.1 Security Overview.doc	AVC Edge Security Overview Release 4.1
AVC Edge 4.1 System Software Spec.doc	AVC Edge System Software Specification Release 4.1
AVC Edge 4.1 System Hardware Spec.doc	AVC Edge System Hardware Description Release 4.1
AVC Edge 4.1 Technical Spec.doc	AVC Edge Software Technical Description Release 4.1
	Sequoia's response to State of Ohio RFP Number SOS0428365

Continued on the next page

File Name if Electronic	Document Title or Description
Other	
InfoSENTRY_Comments_on_Compuware_Template_20031016.doc	InfoSENTRY, Comments on the Compuware Template, October 16, 2003
Recommended Changes_Security Doc102803-InfoSENTRY.xls	InfoSENTRY, Requirements Document Recommended Changes, October 28, 2003
Report to the Ohio Secretary of State from RJVC.doc	RJV, Report to the Ohio Secretary of State, Voting System Vendor Information Review, August 15, 2003
(n/a)	Voting System Vendor Information System Security Review, 08 August 2003
Evaluation Findings Report_09102003.pdf	Vendor Proposal Evaluation Findings Report & Addendum, Statewide Voting Systems, Report Date August 15, 2003, Addendum Date September 10, 2003
State Plan.doc	Changing the Election Landscape in the State of Ohio, A State Plan to Implement the Help America Vote Act of 2002 in Accordance with Public Law 107-252, §253(b), May 13, 2003
HavaRFP5-22-03.doc	State of Ohio Request for Proposal for Statewide Voting Systems, RFP Number SOS0428365, May 23, 2003
N/A	Schneier, Applied Cryptography - Protocols, Algorithms, and Source Code in C, Second Edition
SAIC-MD voting system report final.pdf	SAIC, Risk Assessment Report, Diebold AccuVote-TS Voting System and Processes, September 2, 2003
votingsystemreportappb.pdf	Appendix B: Security Statements from the Rubin Report & State of Maryland Controls
voting_system_security_action_plan.pdf	State of Maryland, Diebold AccuVote-TS Voting System Security Action Plan, September 23, 2003
Source: Internet location http://avirubin.com/vote.pdf.	Analysis of an Electronic Voting System, by Aviel D. Rubin *et al*, July 23, 2003
Security Assessment Scope.doc	Scope Statement, Statewide Voting Systems Security Assessment
sos_testing_final.doc	Compuware, Proposal for the Direct Recording Electronic (DRE) Voting Machine Security Assessment, September 15, 2003
Sp800-30.pdf	Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-30
(n/a)	The Capability Maturity Model, Guidelines for Improving the Software Process, by Carnegie Mellon University Software Engineering Institute