SysTest Labs
216 16th Street • Suite 700
Denver, Colorado 80202
tel: 303/575-6881 • fax: 303/575-6882
www.systest.com

SysTest labs

Consulting and Testing Services

Risk Assessment Study of Ohio Voting Systems

Technical Report

Developed for:

State of Ohio
Secretary of State

Document Number SL-OH-TECH-FRPT-01

TABLE OF CONTENTS

List of Tables

1. INTRODUCTION: EVEREST PROJECT

The Ohio Voting System Risk Assessment was intended to independently assess the risk that the State of Ohio electronic voting processes and systems will operate reliably and produce accurate results. SysTest Labs' areas of assessment on each of the three (3) State of Ohio certified voting systems were:

a. Configuration Management

b. Election Operations and Internal Controls

c. Performance Testing

These systems include Election Management software, Direct Recording Electronic systems (DRE), Optical Scan systems, and Ballot Marking systems with trusted software builds, as noted below.

Vendor	**System**	**Description**	**Model #**	**Software/ Firmware Version**
ES&S	Unity	Election Management software		3.0.1.1
	Automark	Ballot Marking System	87000	1.1.2258
	iVotronic	Voter Dre	90998-BL	9.1.6.4
	iVotronic	Supervisor DRE	91057-BL	9.1.6.4
	iVotronic	ADA DRE	93038-BL	9.1.6.4
	Model 100	Tabletop Opt Scan Counter	76102B	5.2.1.0
	Model 650	High Speed Opt Scan Counter	50650	2.1.0.0
Premier	GEMS	Election Mangement software		1.18.24
	TSx	Voter DRE	TSx	4.64
	Accu-Vote 2000	Tabletop Optical Scan Unit	AVOS	1.96.6
	AccuVote OS Central Count	High Speed Optical Scan Unit	AVOS	2.0.12
	VC Programmer	Hardware for programming key cards	ST100	4.6.1
	Key Card Tool	Software for programming key cards		4.6.1
Hart	Ballot Origination, Tally, Rally &	Election Management Software Components		

Vendor	System	Description	Model #	Software/ Firmware Version
	Servo			
		BOSS		4.3.13
		Tally		4.1.10
		SERVO		2.3.7
		Ballot Now		3.3.11
		eCM Manager		1.1.7
	e-slate	DRE	e-slate 3000	4.2.13
	e-scan	Precinct Opt Scan Counter	e-scan	1.3.14
		Judges Booth Controller		4.3.1
		Verifiable Ballot Option (VVPAT)		1.8.3

1.1 General Assessment Information

1.1.1 Configuration Management

The SysTest Labs Risk Assessment Team performed a Physical Configuration Audit and reviewed supporting documentation for each of the manufacturer’s voting systems installed at the State of Ohio Computing Center in Columbus, Ohio. The purpose of the audit was to verify that the configurations of the sample systems, as defined by the hardware, firmware and software revision levels, was on the State of Ohio’s list of certified systems.

In addition, the SysTest Labs team assessed the processes and procedures used by the State of Ohio to manage the equipment configuration in the field. Of particular interest were the configuration management practices for ensuring that the equipment was at the proper certified level and how updates and upgrades are managed and controlled.

SysTest Labs also conducted a review of the Logic and Accuracy (L&A) procedures in use by a select set of eleven (11) counties (specific counties were selected by the Secretary of State). We particularly looked for consistency across the State of Ohio certified and deployed vendors’ equipment and if the procedures included steps for the verification, both before and after an election, of the hardware, firmware and software versions in use by the counties.

1.1.2 Elections Operations and Internal Control Assessment

The objective of the Election Operations & Internal Control Assessment was to determine whether existing or proposed policies, procedures, internal controls established in existing Vendor documentation and County practices are sufficient to ensure secure and accurate elections based upon software, hardware and operational vulnerabilities identified during previous and current testing phases. Our approach to this aspect of the risk assessment activity is much broader than may be used in other phases of the project. Risks to elections operations and internal controls, in our view, includes any action (or inaction) that has the potential to adversely impact the accuracy, timeliness and transparency of an election beginning at candidate filing through recounts, but with emphasis on voting systems.

SysTest Labs team took a holistic approach to this assessment, addressing the entire election process of which voting systems are one singular component, albeit the most visible one. The research effort has included on-site interviews and assessments that have focused on internal control operational policies, procedures and processes which a representative sample of Ohio counties employ and the impact they have overall on security. Additionally we have included a review of Vendor documentation provided in support of the various voting platforms in use throughout Ohio.

SysTest Labs supports the understanding that a voting system is part of a larger process, and that well implemented security and operational policies, procedures and processes can significantly reduce any level of risk, much of which must be developed locally to reflect not only the specific voting system platform, but the unique nature of the environment in which the system is used. This is consistent with our view that the greatest risks to the voting process and the integrity of elections are not created by voting technology but rather by management practices, operational constraints, inadequate funding and resources, regulatory frameworks as well as less than helpful/useful Vendor documentation.

It is important to note that many risks to elections originate from poor management practices, inadequate training, complex and voluminous Vendor documentation, human error, unnecessarily complex and cumbersome laws and regulations, inadequate funding and resources, and partisan advantage. Many of these effect the ability of the election community, i.e., local election officials, state election officials and legislative bodies, to be effective in preparing for and running an election..

Other assessments have focused, and continue to focus on external threats to voting technology which may or may not have merit. The solutions to election administration issues, voter confidence and the security and integrity of elections are not to be found solely in the technology. Regardless of the thoughtfulness and thoroughness of a design, the complexities and cost associated with creating systems that are 100% secure solely on their own is unrealistic. True security is a combination of technology related security techniques and security measures found in thoughtful, well documented policies, procedures and processes for internal controls that are reflective of both a specific locality and a specific voting system.

1.1.3 Performance and Usage Testing

The purpose of the Performance Testing portion of the risk assessment was to determine if there were any risks to the integrity of an election and accuracy of the vote counts when using each of the certified voting systems as defined by the Vendor documentation for normal usage. SysTest Labs developed a Performance Test Plan and associated Test Cases that defined the approach the Test Team used to provide the State of Ohio Secretary of State (SOS) with performance testing on the Unity, GEMS, and Ballot Origination, Tally, Rally & Servo Voting Systems developed by ES&S, Premier, and Hart InterCivic respectively.

SysTest Labs performed:

1. Usability tests as defined in the EAC guidelines; however, these did not include ballot layout and disability testing
2. Volume testing to verify that at capacity a warning or error message alerted the poll worker to ensure the system does not overwrite existing data
3. Performance testing to ensure that votes are counted accurately and completely
4. Compatibility testing to verify that PCMCIA cards and the EMP card reader failure is discovered and mitigated
5. Verification testing to ensure VVPAT mechanisms is in place to assure a valid paper record is produced for privacy, auditing, verification, and recording accuracy of the ballot casts.

SysTest Labs developed a Performance Test Plan that defined the approach the Team used to implement performance testing on the Unity, GEMS, and Ballot Origination, Tally, Rally & Servo Voting Systems developed by ES&S, Premier, and Hart InterCivic.
The Test Plan was reviewed and approved by the Secretary of State's Office.

1.2 Purpose

This document is the EVEREST Project Technical Report Report. This report was developed as a granular review of the project's minor through critical findings, with specific technical details.

1.3 Statement of Independence

SysTest Labs Incorporated is technically, managerially, and financially independent from all electronic voting systems vendors as specified in *IEEE 1012-2004* Annex C. SysTest Labs has established a policy to ensure independence from companies whose projects are under analysis or assessments by SysTest Labs. The policy is as follows:

The management and staff of SysTest Labs shall maintain an independent decisional relationship between SysTest Labs and its clients, affiliates, or other organizations so that SysTest Labs' capacity to perform risk assessment services objectively and without bias is not adversely affected.

SysTest Labs shall maintain independence in fact and in appearance from clients whose projects are or are scheduled to be under analysis or assessments by SysTest Labs. Control of the project budget shall be vested in an organization independent to all parties. The risk assessment environment, whether on-site at SysTest Labs or at a client's site, shall be organized so that staff members are not subjected to undue pressure or inducement that might influence their judgment or the results of their work.

1.4 References

1. Election Assistance Commission Voting System Standards (EAC VSS), 2002 Version 1.0. Volume I and II.
2. Election Assistance Commission Voluntary Voting System Guidelines (EAC VVSG), 2005 Version 1.0. Volume I and II.
3. Draft Election Assistance Commission Voluntary Voting System Guidelines, 2007 Version 1.0. Volume I and II.
4. SysTest Labs Quality System Manual, Revision 01, prepared by SysTest Labs
5. NIST Special Publications 800-30, Risk Management Guide for Information Technology Systems, July 2002
6. See also section 1.6 for a list of vendor deliverables.

1.5 Systems Information

Items identified in Table 1 - Matrix of Required Software reflect all software required for configuration management assessments and for execution of all performance tests.

Table 1 - Matrix of Required Software

Vendor	**System**	**Description**	**Software/ Firmware Version**
ES&S	Unity	Election Management software	3.0.1.1
	EDM	EMS Database	7.4
	AM	Security and User Tracking for EDM	7.3.0.0
	ESSIM	Publishing tool for printing ES&S paper ballots	7.4
	iVIM	Publishing tool for graphic ballots for iVotronic Precinct Voting Systems	2.0
	HPM	Export the election definition for use in the voting terminals and scanners and reporting module.	5.2
	ERM	Results Reporting Program	7.1.2.0
	DAM	Transfers results to central collection location	6.0
Premier	GEMS	Election Management software	1.18.24
	Key Card Tool	Software for programming key cards	4.6.1

Vendor	System	Description	Software/ Firmware Version
Hart InterCivic	Ballot Origination, Tally, Rally & Servo	Election Management Software Components	
	BOSS	Ballot Creation	4.3.13
	Tally	Tabulation and Reporting	4.1.10
	SERVO	Equipment and Data Management	2.3.7
	Ballot Now	Ballot Printing and Central Scanning	3.3.11
	ECM Manager	ECM Manager	1.1.7

Equipment identified in Table 2, Table 3, and Table 4 reflects all hardware required for configuration management assessments and execution of all performance tests.

Table 2 - Matrix of Required Hardware, Premier

Premier System	Description	Manufacturer	Model	Hdwe Version	Software Version
GEMS Server PC	PC (Personal Computer)	DELL	1800, 2800, 2900	N/A	N/A
TSx DRE	Voter Terminal	Premier	AVTSx	00-103380-000B	4.6.4
TSx printer	VVPAT thermal printer		AVPMX	00-105514-000A	3.0.3
TSx PCMCIA Cards	128MB card	COTS			N/A
Accuvote Precinct Scanner	Table Top Ballot Scanner	Premier	AVOS 79811-04	00-103384-000D	1.96.6
Accuvote Central Scanner	Table Top Ballot Scanner	Premier	AVOS 79811-04	00-103384-000D	2.0.12
Accuvote Memory Card	128KB memory card				N/A
Ethernet Switch Or Hub	Connectivity device	COTS (3Com)		N/A	N/A

Premier System	Description	Manufacturer	Model	Hdwe Version	Software Version
Port Server	Connects serial port to RJ45 ports	COTS (DIGI)	Port Server II 16	N/A	N/A
EMP Server PC	PC (Personal Computer)	DELL	3100		Windows XP SP2
Election Media Processor (EMP)		Premier	A, B, C, D EMPD-GS	111141-200D	4.6.2.0
Key Card Reader/Writer	Smart card terminal	COTS (SmartTech)	ST-100	N/A	N/A
Label Printer	COTS (Dymo)	Dymo	93089	N/A	7.5.0.9
Express PollBook 5000	Voter registration terminal	Premier	2000	1.0500.207	2.1.1
Voter Access Card	Voter access memory smart card		VCG, SCG, ACG	DESI1642-1123 vCG SU004KC0/T=0B	N/A
Voter Card Encoder		Premier			1.3.2

Table 3 - Matrix of Required Hardware, Hart InterCivic

HART System	Description	Manufacturer	Model	Hdwe Version	Software Version
BOSS Server	PC (Personal Computer)	DELL (software must be installed by vendor)			Windows 2000 SP4
Optional SERVO Laptop	PC (Personal Computer)	DELL (software must be installed by vendor)			
eSlate (DRE)	Voter Terminal	HART	3000		4.2.13
eScan	Table Top Ballot Scanner	HART			
Judges Booth Controller (JBC)	Supervisor Terminal	HART	JBC 1000B		4.3.1

HART System	Description	Manufacturer	Model	Hdwe Version	Software Version
Audio card	Disabled Access Unit (DAU) card for audio recording				N/A
PCMCIA Cards (MBB)					N/A
Verifiable Ballot Option (VBO) Printer	Voter Verifiable Paper Audit Trail (VVPAT) Printer	HART	VBO		1.8.3
Syprus USB Removable Media Key (eCM)	USB	SYPRUS		N/A	
ATA Card Reader/Writer	Used To Read Flash To Read/Write PCMCIA Cards	Flash Reader	UISA2SE		
Ballot Box	Holding device for scanned ballots from the eScan unit	HART		N/A	N/A

Table 4 - Matrix of Required Hardware, ES&S

ES&S System	Description	Manufacturer	Model	Hdwe Version	Software Version
iVotronic (DRE)	Voter DRE	ES&S	iVotronic DRE	1.1	9.1.6.4
iVotronic (DRE)	Supervisor DRE	ES&S	iVotronic DRE	1.1	9.1.6.4
iVotronic Compact Flash	CF Memory Card	COTS (SanDisk)	SDCFJ	N/A	N/A
Precinct Ballot Counter	Table Top Optical Scanner	ES&S	M100	N/A	5.2.1.0 BIOS 2.02
Central Ballot Scanner	High Speed Optical Scanner	ES&S	M650	N/A	
Line Printer		COTS (Okidata)	Microline 520	N/A	N/A
Automark Voter Assist Terminal (VAT)	Ballot Marking System	Automark	A100-00	N/A	
Automark Compact Flash	CF Memory Card	COTS			N/A

ES&S System	Description	Manufacturer	Model	Hdwe Version	Software Version
Real-Time Audit (RTAL) Log Printer	Voter Verifiable Paper Audit Trail (VVPAT) Printer	ES&S	PSA-80H-DRE	N/A	011
Personalized Electronic Ballot (PEB)		ES&S	91747-iV1.7c-PEB-S	N/A	N/A
Communication Pack	Printer And Communication Modem	ES&S	91756 iV1.2-CP	N/A	N/A
Printer	Seiko printer used for printing zero tapes etc.	Seiko	SII DPU-3445	N/A	N/A
Ballot Box	Holding device for scanned ballots from the M100	ES&S		N/A	N/A

1.6 Deliverable Materials

In addition to the hardware and software identified in section 1.5, ES&S, Premier, and Hart InterCivic delivered the following documents as a part of the Unity, GEMS, and Ballot Origination, Tally, Rally & Servo Voting System respectively.

1. ES&S

- Unity Data Flow Process
- Unity Overview Table
  - EDM Data Sheet
  - BIM Data Sheet
  - iVIM Data Sheet
  - HPM Data Sheet
  - DAM Data Sheet
  - ERM Data Sheet
- ES-AM Software spec 7.3.0.0
- ES-DAM 6.0
- ES-DAM functional spec 6.0 _11-9-05_
- ES-EDM 7.4 ed for Unity 3.0.1.0
- ES-EDM functional spec 7.3
- ERM 7.1.0.0 for Unity 3.0 final FOR CERT
- ERM Software Specifications 7.1.0.0
- ES-ESSIM 7.4 ed cm
- ITA ESSIM 7.3.0.0 Functional spec
- HPM 5.2.3.0 for Unity 3.0.1.0
- HPM Software Specifications 5.2.0.0
- Ivim install doc
- iVotronic Image Manager 2.0
- System 3.0.1.1 TDP

2. Hart InterCivic

- Operations Manuals

  - BalNow6100-067_Rev33-62A
  - BOSS6100-019_Rev43-62A
  - Rally6100-114_Rev23-62A
  - SERVO6100-102_REV42-62A
  - Tally6100-049_43-62A
- Technical Specs
  - Ballot Now Functional Specification
  - BOSS Functional Specification
  - eCM Manager Functional Specification
  - eScan Functional Specification
  - eSlate_FuncSpec
  - JBCFuncSpecB
  - ServoFunctionalSpec
  - Tally Functional Specification
  - VBO Functional Specification
  - System 6.2.1 TDP

3. Premier

- AccuView_Printer_Module_Hardware_Guide_Revision_3.0
- AccuVote-OS_Central_Count_2.00_Users_Guide_Revision_4.0
- AccuVote-OS_Hardware_Guide_Revision_10.0
- AccuVote-OS_Pollworkers_Guide_Revision_3.0
- AccuVote-OS_Precinct_Count_1.96_Users_Guide_Revision_4.0
- AccuVote-OS_Service_Guide_Revision_1.0
- AccuVote-TSx_Hardware_Guide_Revision_11.0
- AccuVote-TSx_Pollworkers_Guide_Revision_6.0
- AVPM_Service_Guide_Revision_1.0
- AVPM_Single_Roll_Opening_and_Closing_Procedures_Revision_3.0
- Ballot_Specifications_Revision_3.0
- Ballot_Station_4.6_System_Administrators_Guide_Revision_3.0
- Ballot_Station_4.6_Users_Guide_Revision_2.0
- Client_Security_Policy_Revision_6.0
- Election_Media_Processor_4.6_Users_Guide_Revision_2.0
- Election_Media_Processor_Hardware_Guide_Revision_3.0
- Express_Poll_Administrators_Guide_for_Versions_2.0_and_2.1_Revision_1.2
- Express_Poll_Emulator_and_Resource_Guide_for_Versions_2.0_and_2.1_Revision_2.0
- Express_Poll_Users_Guide_for_Version_2.0_and Higher_Revision_2.0
- GEMS_1.18_Election_Administrators_Guide_Revision_10.0
- GEMS_1.18_Product_Overview_Guide_Revision_6.0
- GEMS_1.18_Reference_Guide_Revision_8.0
- GEMS_1.18_Results_Server_File_Format_1.1_Revision_1.0
- GEMS_1.18_System_Administrators_Guide_Revision_6.0
- GEMS_1.18_Users_Guide_Revision_12
- GEMS_Ohio_Results_Export_Format_1.0_Revision_1.0
- GEMS_Server_Configuration_Guide_Revision_10.0
- JResult_Client_1.1_Users_Guide_Revision_2.0
- Key_Card_Tool_4.6_Users_Guide_Revision_4.0
- TSText_4.1_Reference_Guide_Revision_2.0
- VCProgrammer_4.6_System_Administrators_Guide_Revision_1.0
- VCProgrammer_4.6_Users_Guide_Revision_1.0
- Voter Card Encoder Installation Guide Revision 1.0
- Voter_Card_Encoder_1.3_Users_Guide_Revision_2.0
- System 1.18 TDP

2. METHODOLOGY OVERVIEW

SysTest Labs' ATOM™ Methodology is a systematic quality assurance and assessment approach that has been audited and approved as the methodology to be used when conducting Voting System Test Lab Certification Testing of electronic voting systems for the Election Assistance Commission (EAC). In addition, SysTest Labs uses ATOM™ in all QA, IV&V, Risk Assessment, and software test engineering efforts for commercial clients, as well as state and Federal agencies.

The EVEREST Risk Assessment effort by SysTest Labs focused primarily on the tasks of analyzing the following:

- Election Process Workflows
- Election Training plans and materials
- Electronic Voting systems deployment plans
- Electronic Voting systems security plans
- Configuration Management of systems Hardware
- Configuration Management of systems Software
- Configuration Management of systems Firmware
- Voting System Performance, i.e., functionality, reliability, usability, security, and accuracy, of the three deployed electronic voting systems

SysTest Labs has observed, monitored, and reviewed pertinent county and vendor activities throughout the project. To facilitate the accomplishments of the risk assessment objectives, SysTest Labs required support from the Secretary of State's staff, county BOEs, and the vendors to gain a sufficient understanding of the election systems as delineated in the State of Ohio Election Statues.

2.1 Election Operations and Internal Controls

The information required to evaluate the effectiveness of operational procedures and controls for voting systems in a potentially high risk environment was collected using three research techniques: surveys, site visits and document review. Eleven counties were selected as a representative sample of Ohio jurisdictions based upon size, demographics and voting systems to participate in the survey and site visit phases of the project. The counties are: Allen, Belmont, Cuyahoga, Fairfield, Franklin, Hamilton, Jackson, Licking, Lorain, Montgomery and Warren.

2.1.1 Surveys

Written surveys, instructions and an introductory letter from the Secretary of State were hand delivered to each of the participating counties on October 2, 2007. The survey and instructions are found in Attachment A to this report. Every county responded to the survey and the responses have been reviewed and incorporated into this analysis.

2.1.2 Site Visits

Each of the selected counties was visited and interviewed by the SysTest Labs team to assess facilities, access controls and physical security. Additionally, election setup, programming and testing processes were reviewed for paper and electronic voting systems. Ballot security, accountability, tabulation, reporting and reconciliation processes were reviewed during the interviews. Election Day procedures for detecting and resolving machine security and operational issues and the corresponding poll worker training and procedures were discussed and assessed. An outline of potential items of discussion during the site visits is found in Attachment B.

Each site visit consisted of a tour of the facilities and a free flowing discussion on the relevant items on the interview outline. As the purpose of the site visits and interviews was not to evaluate each county but rather to determine the type, scope, scale, consistency and adequacy of internal controls and operational practices at a statewide level, notes were not made specific to each county's practices to protect the integrity and effectiveness of security measures and controls each county has in place.

The counties were visited on the following dates:

County	Date
Allen	Oct 26, 2007
Belmont	Oct 19, 2007
Cuyahoga	Oct 18, 2007
Fairfield	Oct 10, 2007
Franklin	Oct 28, 2007
Hamilton	Oct 25, 2007
Jackson	Oct 22, 2007
Licking	Oct 11, 2007
Lorain	Oct 17, 2007
Montgomery	Oct 24, 2007
Warren	Oct 25, 2007

2.1.3 Vendor Documentation

As part of the EVEREST Project – Ohio Voting System Election Operation and Internal Control Assessment a review of voting system vendor documentation was performed. The review of these documents was intended to assess: 1) the level of thoroughness and usability of the documents relative to voting system operations with specific focus on security and election accuracy; and 2) how well county instituted policies, procedures and processes reflected the recommendations of vendors for such activities as identified in their documentation.

Documentation reviewed included:

ES&S –

- AutoMark Poll Workers Guide
- ES-EDM 7.4 ed for Unity 3.0.1.0
- iVotronic 9.1 Operator’s Manual for Unity

Hart –

- 6300-001 62E eSlate M&T #184
- 6300-002 62C BOSS #146
- 6300-003 62C Ballot Now #142
- 6300-004 62B Rally #70
- 6300-005 62C Tally #186
- 6300-006 62C Support Procedures #392
- 6300-131 6.2A VBO EV Standard #74
- 6300-132 6.2A VBO ED Standard #72

Diebold –

- AccuVote-OS Central Count 2.00 Users Guide Revision 4.0
- AccuVote-OS Pollworkers Guide Revision 3.0
- AccuVote-OS Precinct Count 1.96 Users Guide Revision 4.0
- AccuVote-OS service Guide Revision 1.0
- AccuVote-TSx Pollworkers Guide Revision 6.0
- Ballot Specifications Revision 3.0
- Ballot Station 4.6 Users Guide Revision 2.0
- Client Security Policy Revision 6.0
- Election Media Processor 4.6 Users Guide Revision 2.0
- Express Poll Administrator Guide for Versions 2.0 and 2.1 Revision 1.2
- Express Poll Emulator and Resource Guide for Versions 2.0 and 2.1 Revision 1.2
- Express Poll User Guide for Version 2.0 and Higher Revision 2.0
- GEMS 1.18 System Administrators Guide Revision 6.0
- GEMS 1.18 User Guide Revision 12
- JResults Client 1.1 Users Guide Revision 2.0
- Key Card Tool 4.6 Users Guide Revision 4.0

Note: Not all vendor documentation was available in time for appropriate review during the project, in particular ES&S iVotronic documentation.

2.2 Configuration Management

The SysTest Labs Configuration Management Risk Assessment Team reviewed available documentation and performed a Physical Configuration Audit of a voting system installed at the State of Ohio Computing Center in Columbus, Ohio. In addition, the SysTest Labs team assessed the processes and procedures used by the State of Ohio to manage the equipment configuration in the field, as well as, conducting a review of the Logic and Accuracy (L&A) procedures in use by these select counties. We particularly looked for consistency across the State of Ohio certified and deployed vendors' equipment and if the procedures included steps for the verification of the hardware, firmware and software versions in use by the counties.

2.3 Performance Testing

As a separate deliverable to the SOS, SysTest Labs' Performance Test Team developed a voting system specific Performance Test Plan. This Performance Test Plan outlined the approach SysTest Labs implemented to provide the SOS with effective performance testing on the Unity, GEMS, and Ballot Origination, Tally, Rally & Servo Voting Systems developed by ES&S, Premier, and Hart InterCivic respectively. The purpose of the plan was to provide a clear and precise outline of the test elements required to ensure effective Performance Testing. The test plan:

- Identified items that need to be tested;
- Defined the test approach;
- Identified required hardware, support software, and tools to be used for testing; and
- Identified the types of tests to be performed;

The following list of performance test cases were used to confirm the required functionality, accuracy, and reliability of the voting systems.

Table 5 - Matrix of System Level Testing:

Test Cases	Description
TC0010 - Election Creation	The object of this test case is to observe the difficulty or ease of creating an election.
TC1010 - Set-Up and Closure of the Polling Place	The object of this test case is to observe the difficulty or ease of conducting the 'Set up' of the election system at the County and polling station, loading the election, opening the polls and closing the polls.
TC2010 - Configuration Management	The object of this test case is to verify SW and HW versions of the Election system used in testing
TC3010 - DRE Functionality	Verify core functionality of DRE to perform administrative duties
TC4010 - Election Vote Consolidation (Primary & General)	The objective of the Election Vote Consolidation (Primary & General) test case is to verify that vote totals obtained from each

Test Cases	Description
	type of supported voting device (optical scan or DRE) can be accurately consolidated into a central count vote total that all required reports and audit records can be viewed and/or produced.
TC4050 - VVPAT Accuracy	The objective of this test is to test and verify both the functionality and accuracy of the VVPAT printer device associated with a DRE polling place device. The test will confirm that all vote selections are accurately captured on the printer paper, that they are readable, that they can be canceled and changed, and that all changes are accurately reflected on the VVPAT.
TC5010 - Load Test Early Voting	The objective of this test case is to verify votes are not lost due to memory leak while casting ballots in Early Voting Mode on the DRE and exceed its memory capacity via the vendor's automated process or manual input. In addition, verify the Accuracy and integrity of the tally and a warning message is given to the user.
TC5020 - Load Test DRE	The objective of this test case is to verify votes are not lost due to insufficient memory capacity while casting ballots on Election Day Mode on the DRE devices.
TC5030 - Load Test Optical Scan	The objective of this test case is to verify votes are not lost due to insufficient memory capacity while casting ballots on Election Day Mode on the optical scan devices.
TC5040 - Load Test Storage Components	The objective of this test case is to verify a warning message is given to the user when user attempts to load an election definition that exceeds the memory capacity of the external memory device.
TC6010 – Security	The objective of this test case is to verify the Election System will log any unknown external devices that were inserted in any open port of the Election System.
TC7010 - PCMCIA Card Batch testing	The objective of this test case is to verify all PCIMIA cards provided for testing will function according to system specifications. This test case is a result recent problem with Card formatting using the incorrect FAT files.
TC8010 - Audit Tape	The objective of this test case is to verify the Election System will log all activities on each component of the System (Server, DRE, Scanner etc…)

See Table 21, Capacity Testing Matrix Constraints

3. Results of the Review

The purpose of SysTest Labs' efforts in the Ohio Voting Systems Risk Assessment for the EVEREST Project was to identify risks to the accuracy of election results due to error or fraud; determine if any significant risks of accidental or intentional catastrophic machine failure or unrecoverable error exists; identify risks that cannot be sufficiently mitigated, indicating inherent system inadequacy; and discuss improvements that are required to maximize election integrity. SysTest Labs has developed a comprehensive set of all risks identified as a result of this assessment and have documented these in the Technical Final Report. However, in this Executive Summary, we are discussing only those critical risks that have been identified in the assessment.

3.1 Risk Classification Process

The SysTest Labs risk assessment process uses a combination of the probability of occurrence and the impact of the occurrence, should it occur, to assess the risk. These factors depend on an analysis of both qualitative and quantitative data. For example, qualitative data sources can be based on the experience of team members at the time the risk is identified because experienced staff is sensitive to routine pitfalls. On the quantitative side, the risk assessment may depend on an analysis of more concrete data such as budget and cost information. This data gathering is part of the risk assessment activity. As noted in Table 6 Risk Assessment Classification, our process identifies both the likelihood and its potential impact.

Table 6 Risk Assessment Classification

Probability of Occurrence	System Impact			
	1 – Catastrophic	2 - Major	3 - Minor	4 – No effect
A	1A	2A	3A	4A
B	1B	2B	3B	4B
C	1C	2C	3C	4C
D	1D	2D	3D	4D
E	1E	2E	3E	4E

Red indicates an unacceptable risk; one that the SysTest Labs Team highly recommends to be addressed

Yellow indicates a risk that may be acceptable but requires a decision

Green indicates an acceptable risk

Table 7 Definition of Likelihood of Risk

Level	Likelihood	Definition
A	Frequent	Likely to occur frequently
B	Probable	Likely to occur several times in the life of the software
C	Occasional	Likely to occur in the life of the software
D	Remote	Unlikely, but possible to occur in the life of the software
E	Improbable	So unlikely it can be assumed the occurrence may not be experienced

Table 8 Definition of Impact of Risk

Category	Title
1	**Catastrophic**
2	**Major**
3	**Minor**
4	**No Effect**

3.2 Election Operations and Internal Controls

3.2.1 Scope and Purpose

SysTest Labs Election Operations and Internal Controls Team's concept of risk assessment is much broader than may be used in other phases of the project. Risk, in our view, includes any action (or inaction) that has the potential to adversely impact the accuracy, timeliness and transparency of an election beginning at candidate filing through recounts, but with emphasis on voting systems. Furthermore, we see risk resulting from vulnerabilities as belonging to two categories; unmitigated and mitigated with unmitigated risk posing the greatest challenge to the integrity of elections. In this regard, the SysTest Labs' approach is unlike previous reports regarding voting system security.

3.2.2 Documentation Analysis

The documentation reviewed by each vendor was focused on operational and security procedures; it was not system specific technical and design documentation. Rather it was user oriented with the emphasis on how each vendor via documentation instructs election officials in preparing, using and securing their respective voting system platforms. Not all documentation was available in time for this report (available documents are listed above in Section 1.7.4).

Each Vendor documentation package evaluated was thorough and comprehensive in nature. However, the level of detail combined with the comprehensive nature of the documentation make utilization of the documents by counties challenging. So much material was provided that the documents are not user friendly – this was reinforced during discussions and interviews with county election personnel. The amount of documentation and its technical complexity makes the documentation less than helpful when information is needed.

The provided Vendor documentation suffices for purposes of Technical Data Packages as identified in the Voluntary Voting System Guidelines, however its value to users is questionable. For the average election administrator, the documentation is a labyrinth of seemingly unrelated and disjointed information which, in the opinion of the SysTest Team, was predicated on misplaced assumptions by the vendors of the levels of technical knowledge and election operations specialization at the user level. While election operations specialization would be the ideal thus making the majority of the vendor documentation which focuses in detail on specific areas of voting system operations very germane, this is not the situation most Ohio counties are faced with at this time. In many of Ohio's 88 counties, only a few individuals are directly involved with voting system operations and these individuals wear many hats for these operations – they are essentially "Jacks of all trades." Thus the type of documentation provided by vendors is as stated thorough and comprehensive, yet in general it remains challenging to effectively and efficiently utilize.

Given the level of technical detail, an issue with all vendor provided documentation is the level of generalization employed. (Note: Exception would be in Premier documentation some references were made to specific requirements of other states, but this was very limited). While the uniformity of documentation is important, it none-the-less does not address the individual uniqueness of a state's respective election code/laws and/or customary practices. Counties in general are left to weed through the voluminous levels of materials to find information which may or may not address a specific challenge unique to that county; while each vendor provides access to customer service or provides account managers, a county may be vying for help during a period in which the resources of the vendor itself is taxed. Quick responses are not the norm. To the most possible extent possible, counties should be self-sufficient for all but the most complex problems.

Useful documentation must be concise, usable and, in the opinion of the SysTest Team, organized along the lines of the overall election cycle in order for a county to achieve self-sufficiency. There is a misperception that the Vendor documentation is a workable substitute for local, documented policies and procedures. Most counties have simply made use of vendor provided documentation and information in development of simple check sheets in lieu of formal documented, county (or state) specific election policies, procedures and processes. This can be particularly problematic given that most election personnel are not voting system technology specialists and may not appreciate some of the underlying subtleties and thus overlook an important step or warning in a process that seems inconsequential but may have direct impact on the overall success of the election.

It should be noted that the Vendor Documentation for this portion of the Everest project was not made available to the reviewers until November 15, 2007 and consisted of 27 discrete documents consisting of over 2200 pages of information; as a result of the time constraints we made a concerted effort to focus our review on corresponding areas of documentation that were part of our interviews and site surveys – to this end, identifying of merit and deficiencies regarding documentation should not taken to be a complete list.

3.2.3 Documentation Areas of Merit

It should be noted that the Vendor Documentation for this portion of the Everest project consisted of 27 discrete documents consisting of over 2200+ pages of information; as a result of the time constraints we made a concerted effort to focus our review on corresponding areas of documentation that were part of our interviews and site surveys – to this end, the identifying of areas of merit and deficiencies regarding documentation should not taken to be a complete list.

3.2.4 Areas of Deficiencies

3.2.4.1 Election Systems & Software

- Only three documents were available to review
- ES&S documentation is a compilation of many disparate systems but together under one umbrella, which makes use in the field by BOE challenging.
- ES&S AutoMark documentation (AutoMark Poll Workers Guide SQS-5061-002-R) is the best and most user friendly of the ES&S provided documentation; it has clearly identified step-by-step procedures which can be successfully implemented
- Access Control procedures for the AutoMark and iVotronic are clearly defined, but are not uniformly utilized throughout the state
- Other provided ES&S documentation is very technical in nature and voluminous; using the documentation as a quick reference guide may (can) prove challenging to the average BOE staff member responsible for creating elections using Unity documentation
- ES&S documentation presupposes a higher than average working knowledge and familiarity with computers and databases – lexicon and terminology is not consistent and an individual not familiar with the nuances of computers may struggle to complete a specific task/assignment
- Local election policies, procedures and processes are cobbled together from multiple documentation sources in an attempt to make coherent and structured

environment; with the nature of the documentation much appears to be left to chance and intuition on the part of counties when using ES&S documentation

- In most instances, ES&S provides too much information to be assimilated by the average BOE staff member; excruciating detail is provided which can bog down an individual in the conduct of an other wise straight-forward task – simple step-by-step procedures are not easily obtained from the existing documentation
- The preponderance of ES&S documentation provided appears to be more oriented towards initial installation and setup rather than ongoing operations; this emphasis adds to the complexity of the documentation
- Sections of documentation regarding Poll Worker Election Day Procedures are very thorough but as previously mentioned included extraneous information which is not necessary and can add a level of complexity and confusion that does not need to be there and can compromise election reliability

3.2.4.2 Premier

- Sixteen documents were available to review – the Express Poll documentation (aka, electronic poll book / roster) was not reviewed in detail as most localities are not using this technology (it is recommended that it be reviewed in detail later as voter check-in is clearly a problematic challenge (provisional voters, voter id, which ballot, etc)
- Premier documentation is much more structured package of information; it is broken into various system components and functionality
- Premier documentation also presupposes a level of technical knowledge that the average BOE staff member may not possess
- Premier documentation is clearly structured based on technical competencies rather election functions – in several areas it is clearly apparent that the documentation is oriented to specific personnel roles which may or may not exist in most localities
- Other provided Premier documentation is very technical in nature and voluminous; using the documentation as a quick reference guide may (can) prove challenging to the average BOE staff member responsible for creating elections using Premier documentation; this was acknowledged during the site visits
- No single document exists within the family of Premier documentation that can be used to quickly, efficiently and effectively construct policies, procedures and processes in the field – extensive cross-referencing is required to complete the average election process and that is dependent on the ability of BOE personnel to find the specific information or instruction needed
- Premier documentation presupposes a higher than average working knowledge and familiarity with computers and databases – lexicon and terminology is not consistent and an individual not familiar with the nuances of computers may struggle to complete a specific task/assignment
- Local election policies, procedures and processes are cobbled together from multiple documentation sources in an attempt to make coherent and structured environment; with the nature of the documentation much appears to be left to chance and intuition on the part of counties when using Premier documentation

- As with ES&S, Premier provides too much information to be assimilated by the average BOE staff member; excruciating detail is provided which can bog down an individual in the conduct of an otherwise straight-forward task – simple step-by-step procedures are not easily obtained from the existing documentation

3.2.4.3 Hart InterCivic

- Eight documents were available to review
- Hart documentation is the most structured package of information reviewed; it is broken into various system components and functionality which generally flow with the nature of the election cycle
- Hart documentation is better written and can be easily understood by most non-technical personnel
- Hart documentation is clearly structured based on non-technical competencies
- Hart documentation as are other vendor documentation packages divided into system functionality; yet while it is easier to navigate than other documentation it is non-the-less very voluminous in nature and challenging to use quickly
- Hart documentation makes extensive use of a variety of check sheets – while these checks sheets are by nature general, they can provide a solid framework for developing county specific policies, procedures and processes which can ensure the success of the election
- The closest document provided by Hart which could act as a single controlling election document is the Hart Voting System Management and Tasks Training Manual; however, as well laid out as it appears to be, the document must still have significant portions extracted and changed to accommodate a specific county – this presupposes a level of technical knowledge which may or may not be available within the county

3.2.5 Threat Analysis

The purpose of this section is to describe and define the threat model and methodology and processes that were used to assess the effectiveness of operational procedures and controls for voting systems in a potentially high risk environment. The operational aspect implies procedures and controls in place at the user (local election official) level rather than procedures and controls at the research and development phases (voting system vendor level).

The conduct of elections consists of two major components; automated voting systems and voting operations and activities. This dual nature of elections is acknowledged in the introductory section of SP 800-30,

> "The principal goal of an organization's risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization." (SP 800-30, p. 1)

The primary reference for voting systems is NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, July 2002. However, the focus on IT and systems limit the utility of SP 800-30 in analyzing vulnerabilities and risks to non automated facilities, equipment and activities.

3.2.6 Key Concepts and Definitions

3.2.6.1 Threat Mitigation Concepts

Vulnerability: An attribute, characteristic of an object (software, hardware or activity) that, if exploited, may compromise or result in the loss of the object or its integrity. **Threat or Threat Actor:** A threat is a person(s) or event that may attempt to exploit a vulnerability. Motive, whether personal gain, maliciousness or simple human error, is an important consideration in identifying potential threats. The access of a threat to the target influences the probability that a vulnerability will be exploited. Additionally, events such as earthquakes, fires, severe weather, etc are also threats to be considered in performing a risk analysis. While there is no malicious motive with these types of events, the resulting loss, damage or compromise of assets is just as real as if human caused.

Threat-action: The identification or presence of a threat does not automatically result in attempts to exploit the vulnerability of an object. The motives of the threat combined with the situational context influence if or when a threat will act.

Controls and Countermeasures: Controls and countermeasures (C&CM) are actions taken to reduce or eliminate the possibility of a threat to successfully exploit a vulnerability. Effective C&CM are developed based upon the nature of the vulnerability and the nature of the potential threat(s). Without a basis in vulnerability and threat, C&CM are costly and ineffective window dressing. C&CM generally fall into one of four escalating categories: deterrence, delay, detection and denial. C&CM may be used interchangeably with mitigation or mitigation strategy.

Risk: Risk is the net negative impact of the exercise of a vulnerability (SP 800-30, p.1). Vulnerability is not risk. It is only potential risk. Risk is not vulnerability’s worst case scenario. It is a variable and calculated value that reflects the probability of a vulnerability being exploited after C&CM have been implemented. Further, risk is categorized into recoverable and non-recoverable sets. Risk can be objectively estimated but the level of acceptable risk is a policy decision by an organization, not an absolute value or scientific fact.

3.2.6.2 Threat Identification

Motivation and the resources for carrying out an attack make humans potentially dangerous threat-sources. Below in Table 9 is an analysis of the types of human threat actors and threat actions that are relevant to a security assessment of voting systems and processes in the US today.

Table 9 Types of Human Threat Actors and Threat Actions

Threat or Threat Actor	Motive	Capability	Threat Actions (examples)	Threat Level
Foreign Governments	Influence election of US Officials, State Officials and/or local Officials	May have virtually unlimited resources, money, technology and agents	-Corrupt key persons, -Blackmail -Exploit technological vulnerabilities -Infiltrate ranks of trusted agents.	According to Federal Intelligence and Law Enforcement agencies, there is no credible threat to elections in Ohio by foreign governments. **Level I**
Voting System Vendors (Management)	Financial gain, ideology, ego	Total access to voting technology from development to implementation and ongoing access throughout the product lifecycle.	-Introduction of Malicious code (e.g., virus, logic bomb, Trojan horse) -Poorly designed systems -Low quality controls -Lack of customer support -Breech of contracts -Fail to gain certification -Refusal to interface with other applications or systems	Malicious code is remote due to Federal and State certification requirements but other threat actions are possible and plausible. **Level II**
Rogue Voting System Programmers	Financial gain, ideology, sloppiness, shortcuts, ego	Access to source code at the application development level.	-Malicious code (e.g., virus, logic bomb, Trojan horse) -Poorly written code -Ineffective code	The actual likelihood of this type of threat is determined by the effectiveness of voting system vendor personnel screening, background checks

Threat or Threat Actor	**Motive**	**Capability**	**Threat Actions** **(examples)**	**Threat Level**
				and operational oversight. **Level III**
Insiders- BOE Staff (non Technical)	Financial gain, ideology, sloppiness, shortcuts, revenge, ego, lack of training	Access to voting data, voting systems, supporting applications and secure areas and sensitive items but not a lot of technical knowledge	-Assault on an employee -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 intrusion -System sabotage -Unauthorized system access	Intentional threat actions are possible but unlikely due to oaths, legal penalties and management and access controls. Given the capability and access, unintentional acts, omissions, errors etc are historically documented threats. **Level II**
Insiders- BOE Technical Staff	Destruction of data, Financial gain, ideology, sloppiness,	Access to voting data, voting systems, supporting applications and secure areas and sensitive items	-Assault on an employee -Blackmail -Browsing of proprietary	Intentional threat actions are possible but unlikely due to oaths, legal penalties and management and access controls. Given the capability

Threat or Threat Actor	Motive	Capability	Threat Actions (examples)	Threat Level
	shortcuts, revenge, ego, lack of training	combined with a high degree of technical knowledge	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	and access, unintentional acts, omissions, errors etc are historically documented threats. **Level II**
Poll/Election Workers	Destruction of data, Financial gain, ideology, sloppiness, shortcuts, revenge, ego, lack of training,	Access to voting machines and ballots prior to and on Election Day, ability to influence and disenfranchise individual or groups of voters	-Improper operation of voting machines -Loss or destruction of ballots, data or equipment -Sabotage of voting process -Voter intimidation -Voter disenfranchisement -Fraudulent voting	Intentional threat actions are possible but unlikely due to oaths, legal penalties and election day oversight. Unintentional acts, omissions, errors, disenfranchisement, etc. are historically documented threats. **Level II**

Threat or Threat Actor	**Motive**	**Capability**	**Threat Actions** **(examples)**	**Threat Level**
	partisanship			
Ballot Printers and Other Election Related Vendors	Financial gain, ideology, Ego, sloppiness, shortcuts, Over-commitment business practices	Source of critical and time-sensitive election material, ability to control quality and accuracy of voting material and services, capable of disrupting entire election process with untimely delivery/service	-Change ballot contents -Incorrectly printed ballots -Improperly finished ballots -Late ballot delivery -Inaccurate voting system database creation -Ballot layout errors -Programming errors -Late delivery of services	Intentional threat actions are possible but unlikely due to professionalism and commitment to voting process. Errors and delays due to business practices, over-commitment of resources, inadequate training, poor quality assurance, miscommunication etc. are historically documented. **Level II**
Legislation, Regulations and Directives	Solve past problems, Partisan advantage, Personal gain or advantage, Response to various interests, Reform	Creates the legal framework and paradigm in which elections are conducted, certified and adjudicated. Touches every aspect of an election.	-Incomplete or vague requirements -Inconsistent or contradictory requirements -Obsolete and outdated requirements not removed when changes occur -Silent on key areas -Focused on past technology and practices -Intent often to satisfy expectations	The threats posed by Legislation, Regulations and Directives are not intentional but result from unintended consequences, omissions, timeliness unmet resource requirements and conflicting directives. **Level II**

Threat or Threat Actor	Motive	Capability	Threat Actions (examples)	Threat Level
			and demands other than effective election administration -Untimely changes during an election -Unnecessary complexity creates additional points of error and failure	
Election Administration and Management practices	Ego, Lack of training, Fragmentation of responsibility, Personal gain, ideology, Partisanship, Favoritism, sloppiness, shortcuts, revenge, ego, Maintenance of Status Quo	Administration and Management practices touch every phase of an election. Poor practices can undermine the security of any voting system and election.	-Arbitrary or inconsistent procedures and practices -Hiring or appointment of unqualified staff -Organization of duties to minimize accountability -Weak or absent oversight -Ineffective planning and management -Reliance on crisis management -Ineffective division of labor and responsibilities -Create high staff turnover rates	Intentional threat actions are possible but unlikely due to professionalism and commitment to voting process. Unintentional threats such as undocumented procedures, errors and delays, inadequate staffing and training, poor quality assurance, mismanagement, miscommunication etc. are historically documented. **Level II**
Activists	Conspiracies, ideologies,	Access to decision-makers and media;	-Cast doubt on integrity of elections	Pose no threat to actual voting system hardware or software

Threat or Threat Actor	**Motive**	**Capability**	**Threat Actions** **(examples)**	**Threat Level**
	political views, personal gain, ego	access to policies and procedures via public disclosure laws.	-Impugn the judgment, character, decisions, practices and policies of election officials -Seek ill-informed but well-intentioned reforms	but may erode voter confidence **Level I**
Political campaigns and Action Committees and Organizations	Election outcomes, Conspiracies, ideologies, political views, personal gain, ego	Access to decision-makers and media; may reveal flaws in policies and procedures via public disclosure laws, recounts and election contests.	-Cast doubt on integrity of elections -Impugn the judgment, character, decisions, practices and policies of election officials -Challenge credibility of specific election outcomes	Pose no threat to actual voting system hardware or software but may erode voter confidence **Level I**
Voters	Misinformation Misunderstanding Mistakes Impatience	Voters are capable of creating confusion locally at a poll on election day, post election source of anecdotal issues or problems	-Questioning reliability of voting machines -Alleging errors -Claims of disenfranchisement -Alleging problems such as delays, lines, improper practices, discrimination	Pose no threat to actual voting system hardware or software but may erode voter confidence and make unsubstantiated claims that cannot be refuted. **Level I**
Fraudulent Voter	Financial gain, ideology,	Capable of attempting fraud, tampering with	-Misrepresenting identity,	Pose little threat to actual voting system hardware or software

Threat or Threat Actor	Motive	Capability	Threat Actions (examples)	Threat Level
	Influence election outcomes ego	machines, disrupting voting at the polls	-Registering multiple times, -Tamper with voting machines, -Voting more than once, -Voting for contests not eligible for, -Creating confusion at polls, -Electioneering	but may introduce illegal votes or influence outcomes on a limited basis. **Level I**

3.2.7 Threat Levels

The threats and threat actors to voting systems and the voting process range from a nuisance level (level 1) to an inadvertent level (level 2) to a malicious level (level 3). Nuisance level threats are characterized by limited time, limited access and limited knowledge and pose minimal risk and impact on an election. This level of threat is easily deterred, detected and isolated and, if it occurs, is limited to a single machine or precinct. Because it is easily detectable, usually correctable and limited in scale, the mitigation strategies to deter, delay, detect and deny a level 1 attack are relatively easy, inexpensive and are not difficult to implement. Generally, such countermeasures and safeguards are technical and are already in place in each voting system. These countermeasures are implemented by local election officials and voting system providers.

Inadvertent level 2 threats are the most frequent and most likely to attack the voting process. Time, access and knowledge available to a level 2 threat may be high or low. Level 2 threats are characterized by lack of training; human error; inadequate quality controls; poor management practices; operational constraints (usually time); budget and staffing constraints; and outdated, incomplete or contradictory regulatory frameworks. The mitigation strategies to deter, delay, detect and deny a level 2 attack are not of a technical nature. They are, in many ways, the most complex, slowest to implement and controversial as they require action from multiple actors at multiple levels. These countermeasures are implemented by state and local legislative bodies, state and local elected officials, state and local election officials as well as voting system providers.

Malicious level 3 threats are potentially the most catastrophic, hardest to detect and the most difficult from which to recover. Fortunately they are also the least likely to attack the voting process. This level of threat is characterized by authorized access, few time constraints and a high level of technical knowledge regarding the voting system or the voting process, in other words, a malicious voting system or Board of Election insider. Because it is difficult to detect and global in scale, the mitigation strategies to deter, delay, detect and deny a level 3 attack are thorny, expensive and are difficult to implement. Countermeasures and safeguards for a level 3 threat may found in technical solutions but are most effectively found in operational and procedural frameworks. These countermeasures are implemented by local election officials and voting system providers.

3.2.7.1 Threat Mitigation Concepts

It is not realistic to attempt to develop mitigation strategies or countermeasures that eliminate entirely any risk posed by any vulnerability. This is true particularly in elections, one of the most human of activities. To eliminate or deny the possibility that any vulnerability in a voting system or voting process could be exploited would require costly and severe limitations on the exercise of the right to vote as historically exercise in our country. Absolute election security would require the sacrifice of the revered secret ballot and would impose draconian identification and other control measures or the elimination of elections all together. Denying a threat the possibility of exploiting a vulnerability is the goal, not the standard of security. Countermeasures and mitigation strategies should seek to eliminate all risk but on the other hand realize that denial is unreasonable, costly and impossible to achieve while retaining the other American values associated with the exercise of democracy.

While denial is the ultimate objective, effective countermeasures and mitigation strategies will seek to develop practices that will deter, delay, and detect attempts at exploiting vulnerabilities. Of these, detection is the most powerful principle as it affords the ability to identify, isolate and recover from attempted breeches of security. These four “D”s are the basis of our approach in identifying and recommending mitigating measures for the vulnerabilities we have identified.

3.2.8 Application of the Threat and Risk Analysis Model

It is with guidance from NIST Special Publication 800-30 and extensive election experience, that the threat and risk analysis process for this Ohio project is focused on potential threats during the operations phase of the system development life cycle (SDLC) (SP 800-30, p. 5). It will focus on the life of the generally understood eight (8) defined states in a voting system election life cycle, as shown in Table 10, and where actual and real electronic and/or physical touch points exist – that is, “what, where, when and how, ” do threats and threat sources manifest in the voting system election life cycle.

Table 10 Voting System Election Life Cycle States

Life Cycle State	Description
State 1: Pre-Election Storage	Secure warehousing operations, system maintenance, system preparation for elections and changes to system hardware/firmware and software provided by the vendor (if such changes have been approved and certified).
State 2: Election Preparation & Setup	A County is responsible for the setup (preparation) of an election using vendor provided systems.
State 3: Election Deployment of voting units.	Trusted County personnel deliver the voting units to the polling locations prior to an election.
State 4: Polling Location Setup (Opening Polls)	This state includes unsealing, setting up, activation and opening polls (voting machines).
State 5: Voting Operations	This state entails providing access to voting systems for the electorate to cast ballots.
State 6: Voting Shutdown (Closing Polls)	This state is where polls are closed (completion of voting), voting machines provide election results and machines are disassembled and prepared for return to warehouse.
State 7: Election Data Transport	Election results from polling locations are sent physically or electronically to a central tabulation point to determine unofficial election results.
State 8: Election Results and Post Election Storage	Unofficial election results are announced on election night. Voting machines are returned to secure warehouse.

3.2.9 Vulnerability Analysis

Based upon the written surveys and the site visits, significant internal controls, security measures and operational procedures are in-place in each of the counties in the sample; the point of failure is the lack of formal documentation. There is a high level of commitment to protecting the voting systems and voting processes in use in each county from real and perceived threats to the integrity of elections. In our view, the policies, procedures and processes are in place to deter, delay, detect and deny most threats to voting systems specifically and the election environment in general.

These vulnerabilities are generally independent of any voting system vendor, voting system or class of voting technology.

In general, there is a wide-range of approaches and capabilities between localities surveyed and visited that should be identified.

Therefore, within a state such as Ohio there are numerous differences in capabilities, approaches, resources, etc., that regardless of current statutory requirements do not result in uniformity in and amongst the counties. Such differences as well as similarities within Ohio are noted below in Table 11. these differences are cited to convey the broad range of situations SysTest Labs encountered. (Note: Items listed in one column are not reflective of one specific locality, but is simply a list of differences in general.)

Table 11 County Demographic Differences

Large heterogeneous voting populations	Vs	Small homogeneous voting populations
Urban	Vs	Rural
Electronic voting machines	Vs	Optical Scan voting machines
3rd Party Drayage	Vs	Sleepovers
Distributed operations	Vs	Centralized operations
Large elections staff	Vs	Small elections staff
Significant poll worker turnover	Vs	Stable poll worker base
3rd Party Voter Registration System (different than provider of voting system)	Vs	Single provider of both Voter Registration and Voting Systems
Personnel assigned to single functional area (e.g., candidate filings and petitions)	Vs	Personnel assigned to multiple functional areas
Republican / Democrat interpersonal relationship challenges	Vs	Highly coordinated / unified Republican / Democrat interpersonal relationships
New Election Leadership	Vs	Stable Election Leadership
Under-documented policies, procedures and processes	Vs	Documented policies, procedures and processes
Highly electronic based security	Vs	Less electronic based security
More rigorous hiring practices	Vs	Less rigorous hiring practices
Automated L&A DRE Testing	Vs	Manual L&A DRE Testing
Rigorous ballot proofing	Vs	Less rigorous ballot proofing
Pre-marked ballot test-deck for optical	Vs	Hand marked ballot test-deck for optical

scan L&A Testing		scan L&A Testing
Highly structured vote reconciliation processes	Vs	Less structured vote reconciliation processes

Conversely, SysTest Labs noted many similarities amongst the counties involved in the process:

- Utilized policies, procedures and processes (regardless of whether they are documented or not)
- Inconsistent poll worker training among counties with similar voting system platforms
- Election Management Systems (EMS) servers and software under positive control by authorized personnel
- No one person is given unencumbered access to EMS servers and software
- EMS servers and software physically under “lock and key” controlled by authorized election personnel
- EMS servers are stand-alone and not networked, either internally or to the public internet
- EMS servers do not have unauthorized third-party applications installed on their hard drives
- Split logins and passwords for EMS server access and EMS software are used
- Vendors are not allowed unmonitored access
- Extensive use of tamper-proof numerical seals and the recording of serial numbers used for validation by election personnel
- External ports on voting machines are physically locked and are sealed and tracked by serial numbered tamper-proof seals
- Process check sheets are used (organically developed)
- Memory devices coded with election setup physically managed by presiding judges
- Memory devices with election results returned by authorized presiding judges
- EMS software initializes memory devices with election codes and serial numbers to prevent the introduction of non-authorized memory devices
- Presiding judges constantly monitor voter activity at voting booths
- Use of absentee ballot stubs and tracking to prevent the introduction of unauthorized ballots

3.2.10 Overall Vulnerability Assessment

No obvious or serious deficiencies in security or operational practices were observed at any county or for any voting system. All counties had comprehensive, yet for the most part undocumented practices and procedures intended to deter, delay, detect and deny any attempted compromise of the voting systems and voting processes. To a reasonably high degree, these practices were consistent across counties and voting systems.

While the size, location and adequacy of facilities varied greatly among the counties, we found, without exception, that counties made the best use possible of their facilities. In every case, counties made attempts to upgrade and improve the physical security of their facilities since the acquisition of new voting systems.

Counties surveyed make good use of the fiscal, staff and time resources available to them. Of particular note during this election cycle, each county successfully managed and overcame potential problems resulting from the delay in state certification of local option measures and the uncertainty surrounding the "on again, off again" state measure.

3.2.11 Areas of Vulnerability

During the review of the surveys and the conduct of the site visits, several potential risk areas were identified. The bases of these risks were practices or observations in more than a single county. Several themes surfaced independent of voting systems, county size and political persuasion. These themes or risk areas that will be discussed were not all present or observed in any one county and, as a result, we did not observe a set of practices that would compromise the security or integrity of elections in any single county. Certainly, if all these observations were present in a single jurisdiction, the integrity of that county's elections would be called into question. The resolution of these risks will contribute to a higher level of security and integrity of all elections in all counties in Ohio. The specific impact of these risk areas on each voting system are analyzed, discussed and mitigation proposed in subsequent Vulnerability and Mitigation tables.

3.2.12 County Documentation

The most significant issue observed by means of the surveys and site visits was the lack of written documentation of election procedures and security plans. While senior management was knowledgeable and conversant of the county's practices, there was, in virtually all cases, no written documentation to support the operations. In several instances, counties rely upon on a single individual to direct all activities in lieu of having written procedures and trained staff. The lack of written policies and procedures is problematic on several fronts. The absence of written policies and procedures:

1. May result in overlooking important steps or practices
2. Often results in inconsistent procedures from one election to the next
3. Promotes a "silo mentality" among staff and inhibits staff training
4. Enables "knowledge is power" gambits
5. Contributes to a lack of continuity when re-organization or staff turnover occurs, particularly at the top of the organization
6. Places the personal judgment and decisions of Directors and staff on trial, rather than the written procedures, in the event of an election contest.

3.2.13 Physical Security

The facilities in which the BOE operate are inadequate to the operational needs and security needs required to conduct secure and transparent elections using any voting technology. Existing facilities, to include recent enhancements, provide minimal physical protection of ballots and voting systems from unauthorized access.

3.2.13.1 After Hours Access

During business hours and when the facilities are occupied, operational procedures and access controls provide appropriate security and prevent unauthorized access to sensitive items and equipment. After hours and when the facilities are unoccupied, most BOE offices are unprotected and unauthorized access may not be prevented or detected. Exterior doors are locked. However, in some cases, the exterior door to the BOE is an interior door of a building. The offices are vulnerable to unauthorized entry because of inadequate key controls, glass paned doors, un-reinforced, and ground level exterior windows. The vulnerability is that, in most cases, there is no means of detecting (real time) unauthorized attempts at entry and there is no means of surveillance to identify perpetrators. Alarms, intrusion detection systems, video surveillance, locking systems as well as low tech upgrades of doors and ground level windows will address this issue. In some cases, the BOE has no control over after-hours access of county facilities. Maintenance and cleaning crews enter at-will, except for those areas requiring dual keys for locks from the Democrat and Republican election officials.

3.2.13.2 Secure Storage

Secure storage areas are constrained by the facilities and result in less than optimum security. Specific situations observed include the co-mingling of voted and non-voted, counted and uncounted ballots. Sensitive items such as ballots, memory cards and voting machines are stored with non-sensitive items such as office and cleaning supplies. In other cases, secure storage areas are shared with other county departments and are uncontrolled by the BOE.

Items requiring segregation, secure storage and inventory controls have not clearly been identified by levels of sensitivity. For example, no distinction is made regarding the sensitivity of un-voted ballots, voted ballots in envelopes, uncounted and voted ballots out of envelopes, counted and voted ballots, and unused ballots resulting in an unnecessary and risky co-mingling of ballots in the same container or storage area with little means of identification. Similarly, few distinctions are made between surplus memory cards, un-programmed cards, programmed but untested cards, and programmed and tested cards. Such distinctions along with appropriate handling guidelines for each category will enhance security, permit more effective use of facilities and minimize opportunities for mishandling sensitive items.

3.2.13.3 Two Key/Password Systems

The two-key and split password security approach to controlling access to sensitive areas, which is predicated on Ohio’s partisan BOE structure, provides a false sense of security and may even undermine security for several key reasons. Access controls employing physical keys rely on strict key control measures to be effective and provide no means of detecting unauthorized access. Multiple keys, the ability to duplicate keys, a lack of physical control of keys, the ability to not engage one of the locks and negating the need for a second key all limit the effectiveness of a two key system. The cumbersome nature of the two-key protocol invites human nature to devise shortcuts that bypass the controls without detection.

In terms of split passwords or logons to control access to automated systems or locking devices, the sheer awkwardness of securely creating and subsequently inputting the codes by two people make it extremely unlikely that the code or password can remain secret for long. Additionally, once access is granted to the system, a user, with appropriate permissions, can compromise the two-person rule by viewing or modifying the password.

Although we have identified deficiencies with the assumptions and practice of two-key procedures, it appears to us that those in a position to bypass the controls to obtain access are those who otherwise would be permitted access and therefore no real breach of security is occurring. While two-person access rules are appropriate in some situations, reliance on a two-key system to control access in this case is cosmetic rather than substantive. All cosmetic security practices create unnecessary opportunities for actions (or omissions) to be misconstrued as security violations.

3.2.14 Partisanship

The unique partisan overlay that characterizes the organization of Ohio county election board organizational structure create several issues that have or could impact the security and integrity of elections. While such a framework has deep roots in the past and has served to address concerns and fears of fraud of yesteryear, its perpetuation in the 21st century with 21st century technology and 21st century election integrity issues may be counterproductive. First and foremost, the bifurcation of the full time organizations and staff by partisan affiliation introduces an implicit message of mistrust of the opposite party and implies that pursuit of partisan advantage in decisions and actions is expected. While concerns of partisan advantage will never be eradicated under any organizational structure, the cost, disadvantages and risks created by the current system are significant.

3.2.14.1 Job Classifications and Hiring Practices

Additionally, we observed that the job classifications, job descriptions and organizational structures had a tendency to satisfy the partisan requirements but did not satisfy the operational needs and demands for conducting elections. This partisan overlay may prevent the hiring of the most qualified person(s) for new and technical positions. Further, without the power to hire and fire common to other government organizations, the ability of management to effectively and efficiently administer elections as well as set and enforce performance standards provides only the illusion of control and accountability in the organization. In some cases, the hiring process was reported to be controlled entirely by political parties or operatives.

3.2.14.2 Background Checks

Our examination of this issue was spurred by an aspect directly related to security. When asked what screening, reference checks and criminal background checks were performed when hiring new staff, counties responded that they were unable to perform any checks due to partisan constraints. This issue is particularly critical in today's environment in which many of the current security concerns involve actions performed by "insiders". Without an ability to screen new hires, particularly to key positions, organizations are vulnerable to the reality, or merely the accusation, of harboring corrupt insiders that compromise elections.

Some reform of the current partisan paradigm could address these security issues while preserving partisan oversight of the elections process at the local level.

3.2.15 Systems Integration

The non-use of workable interfaces between voter registration systems (VRS) and the voting system election management systems (EMS) with the Premier system, and the lack thereof with the ES&S and Hart systems was observed, creating a create potential and unnecessary points of failure in an election. This absence or non-use of these interfaces has resulted in the creation of parallel management of multiple databases which, in turn, requires double entry of the same data, double proofing of the same material and procedures for synchronizing parallel databases in a dynamic environment.

Improper coding of an election, omitting a precinct or group of voters from an election, omitting a candidate or offices, issuing incorrect ballots to voters or incorrectly tabulating votes are all common issues that have occurred across all voting systems. While not "security" issues in a classic sense, these types of errors undermine the accuracy, integrity and confidence of an election even more that potential security breaches. The risk of such errors is greatly compounded when essential election systems do not "talk" to each other.

3.2.16 EMS & Firmware Version Control and Updates

3.2.16.1 Installation

Within the group of counties participating, we conducted extensive questioning regarding changes to election management software and voting system firmware version control and update processes. It became evident that in this area there was a divergence of approaches used throughout the State. It appears that there are two distinct approaches: Large localities received state approved and certified changes directly from their respective vendors; smaller localities received state approved and certified changes from the vendor via Secretary of State Field personnel. In most instances, vendor personnel are conducting the actual updates and/or changes while being supervised and monitored – vendor personnel are not given login or passwords to gain access to the servers and applications. This task of granting access to vendors is performed by authorized county personnel.

3.2.16.2 Software Chain of Custody and Recordkeeping

We observed the validation, authorization and installation of software and hardware changes as a problematic area which we believe should be the responsibility of the State but is being abdicated to the counties who are often ill-prepared or don't have the ability to perform such an operation. Specifically, we did not observe a formal and consistent statewide process for introducing, delivering, installing, verifying, testing, controlling and documenting such software/firmware changes. This is a particularly sensitive issue area given that many scenarios for compromising voting systems involve the introduction of unauthorized software and firmware.

We did not witness any local record keeping of authorized changes to software/firmware. We did not witness or were made aware of post-change installation testing to verifying the working of the changes and/or updates. We were not made of aware any post-election processes to verify software and firmware version (e.g., using SHA-1 Hashing). We asked some respondents "How do you know that the change or update was what was approved by the state?" To a person, the answer was they "did not know". They relied on the trust they had with their respective vendors. While trust of a vendor is laudable, it cannot be the sole factor in determining the validity of the change and/or update.

Given the level of scrutiny of elections throughout the country, we believe this is an area which requires vast improvement. The ability currently of vendors to deliver changes and/or updates directly puts the county, vendor and general public at risk, a risk SysTest Labs believes is unnecessary. The chain of custody relative to the changes and/or updates is questionable. While there have been instances where equipment was found to be down level, i.e., not have the most recent approved updates, we do not believe inappropriate state approved and certified changes and/or updates are or have been delivered, it would be difficult to definitively say this is the case given the current approaches.

3.2.17 Certification of the Ballot

The point in time when the contents of a ballot is set and final is critical to the creation, production and printing of ballots, programming and testing equipment and issuing of ballots to voters. This date is the final milestone for virtually every task and process in an election and all subsequent time-sensitive tasks are dependent on the finalization of the contents of the ballot.

Current law requires the Secretary of State to certify the ballot 60 days prior to an election. Under the best of circumstances, Election Day minus 60 is a late date for such a critical milestone task to be completed. We observed that this deadline was not met for the current election both for state measures and local options. While missing the deadline by several weeks was possibly a one-time event, any delays have serious down-stream implications and rob local officials and their printers of valuable time to ensure the ballots are complete, accurate and available to meet absentee voter deadlines. Delays also directly pushback the beginning of programming and testing of voting machines for logic and accuracy (L&A) which is already conducted on a compressed timeline.

3.2.18 Testing

L&A testing of paper based and electronic voting systems are meticulously being conducted during numerous site visits and followed vendor recommended practices. Those conducting the testing adhered to the prescribed testing protocol. Testing (and proofing), as observed and discussed during interviews, appears adequate to identify major accuracy or logic issues and machine malfunctions.

3.2.18.1 Marking of Test Ballots

While the intent of L&A testing at the counties is to ensure that a ballot layout, specifically certified for an upcoming election, can be accurately read (accuracy), that all ballot positions can be accurately and reliably voted (ballot design logic) and that the votes recorded will be construed (read) and reported as intended. The approach and mindset during L&A testing appears to remain based upon the operating characteristics of punchcard voting systems and is not designed to identify L&A problems or mistakes unique to optical scan or electronic voting. . For example, machine marked optical scan ballots are used exclusively to test paper based systems rather than using test ballots marks with pens and pencils to replicate the marks of voters. In an optical scan paradigm, machine marks are qualitatively different than marks made by voters. Using machine marked ballots exclusively may not reveal read-head calibration or sensitivity issues that could result in undetected misread ballots on Election Day. This shortfall could easily be addressed by including a volume of hand marked ballots and counting a representative sample of test ballots.

3.2.18.2 Testing Scenarios

Another example pertinent to both optical and electronic technologies is a lack of testing all possible overvote and undervote scenarios (such as vote for 2 or 3 type offices). Test ballots and vote scripts were observed to be designed to produce a punchcard type test result pattern rather than testing all possible voting permutations.

It appears that current testing practices have been handed down orally from the previous punchcard systems and have been augmented by vendor training and guidance. Dedication, hard work and repetitive work are substituted for written documentation based upon thoughtful, system-specific considerations which identify proofing/testing timelines, criteria, and methodologies. Enhanced testing protocols would increase the counties' ability to detect and correct errors or attempts at fraud before they are irretrievably introduced into an election.

3.2.19 Absentee Ballots

The recent laws liberalizing the use of absentee ballots have already resulted in a significant increase in volume which, from our experience, will exponentially grow in the next few years. Concurrent with the increase in absentee voters is the addition of vote tabulation machines and processes that are different than those used at polls on Election Day.

The procedures for issuing, handling, tabulation and reconciliation of absentee ballots and "early voting" ballots observed during site visits have not caught up to the changes in law and voting technology. Due to outdated absentee statutes, the lack of written procedures and inexperience in high volumes of mailed ballots, absentee ballot processes have not evolved to meet the new demands and will prove inadequate for volumes anticipated in a presidential election year.

Specific issues observed include:

1. Stub numbers are tracked by voter, both when the ballot is issued and before it is counted, which provides no security value while jeopardizing the voter's right to privacy.
2. The requirement for the stub to remain attached to the ballot to qualify for counting even though the identity of the voter has been established by signature verification results in inconsistent stub policies internally and between counties. This requirement also provides a new opportunity to disenfranchise qualified voters by error or by fraud.
3. Interpretation of prohibitions on tabulating votes prior to the close of the polls and the relationship of tabulation to opening and scanning have led to absentee ballot processing practices and timelines in many counties that will implode with an increase in volume. Some counties perform no absentee processing until the polls open on Election Day.
4. The real or perceived requirement to count and report all absentee ballots on election night is not realistic as volumes increase or without relief on ballot processing timelines. Continuation of such expectations and/or requirements will unnecessarily create the perception of a problem where none exists as absentee volume increases.
5. Procedures for post election reconciliation of absentee ballots do receive the same priority and do not meet the same standards for ballots cast at the polls. As the percentage of ballots cast by absentee increases, the importance of this reconciliation will increase.
6. Exception handling processes, ballot duplication and enhancement processes are not documented and are inconsistent based upon when the exception is identified.
7. The lack of procedures and ballot accountability for in-office absentee voting on electronic machines may create new opportunities for voter fraud.

While these issues are statutory or operational and not directly related to any particular voting system, the adverse consequences of any of these issues will undermine voter confidence and bring scrutiny, correctly or not, on any voting technology involved.

3.2.20 Storage and Transport of Voting Equipment

We observed that counties had a good understanding of the concept of "chain of custody" of voting equipment but the application of the principle varied. In some cases, the chain of custody for voting machines (both optical scan and electronic) began when the machine was tested for the election. In other cases, it began when the equipment was delivered to the drayage company, poll worker or a polling site.

3.2.20.1 Inventories

We are unaware, through observation and interview, of counties maintaining an ongoing, serial number inventory, status, location and chain of custody of voting machines. Counties could tell us how many machines they owned but could not account for any machines other than those assigned to the election. Verified serial number inventories constitute a chain of custody while equipment is in storage. Similarly, the electronic media (memory cards) were not accounted for on an ongoing basis nor were they visibly marked in a manner to identify them as sensitive items. Every county had a surplus of cards but could not provide a count nor account for them through some type of inventory process.

3.2.20.2 Delivery

Delivery practices vary from county to county with some counties employing contracted professional drayage companies (bonded), others use county resources to deliver equipment and others require the Presiding Judges to pick up and deliver the equipment. Any of these three methods could provide adequate means to deter, delay, detect and deny unauthorized access to the machine if security practices are well considered. Appropriate security practices would deter attempts to gain access and tamper with the equipment by visible warnings, would delay attempts by the use of locks, seals and packaging, and would detect attempts of tampering and unauthorized access through the use of tamper-indicating devices and techniques. The absence of a reasonable and cost effective way to completely deny the opportunity for a determined person to gain access to the voting equipment when the equipment is outside the direct control of the BOE should not be the basis of changing current delivery practices provided that there are measures are in place to deter, delay and detect unauthorized access.

3.2.20.3 Security Seals

Generally, the security practices provided the required security; however, inconsistencies and invalid assumptions were observed regarding the use of serial numbered tamper-indicating seals. Specifically, serial numbered tamper-indicating seals were applied to access points for electronic media and poll workers were instructed to verify the presence of the seal but were not asked to verify the serial number prior to putting the machine into operation. Typically, verifying the presence of the seal would be adequate; however, in several jurisdictions Presiding Judges were issued identical seals as part of their Election Day kit. In this case, the serial number, not merely the seal, must be verified in order to determine that the machine has not been compromised. In other cases, poll workers were trained to record the serial number on their accountability paperwork and the serial number would be verified by the BOE staff after Election Day. This practice would detect possible tampering with a machine but only after votes had been cast and reported from the compromised machine.

3.2.21 Election Day Operations

3.2.21.1 Presiding Judge (Pollworker) Training

Ohio BOE's are faced with dynamically changing and evolving mandates such as provisional ballot and voter identification requirements. These and other changes are continuously are being challenged in courts and as a result, a wide-variety of interpretations have resulted even among Ohio counties. As a result, training of Presiding Judges and their ability to successfully handle various voter situations can dramatically impact the view of election success the public and media have regarding elections. Presiding Judges are the front of the election process and as such act as customer services representations for the BOE; their ability to quickly and concisely address the many conflicting and ever changing requirements of the evolving election process makes them a critical success factor in the overall election process. Compounding this challenge is the turnover experienced by counties in their poll workers; some turnover per election can exceed 40%+. SysTest believes that one critical area for the improvement of Ohio's election process is the development of uniform policies, procedures and processes for poll workers, taking into account the specifics of the voting system platforms utilized. Once done, enhanced and robust poll worker training with the ability to measure how well materials are understood and can be executed should also be considered. Most poll worker training is on average 4 hours in length and can not begin until 60 days prior to the election. Many of the interviewed counties attempt to "cram" extensive amounts of complex information into a short period of time. It is the SysTest's team's belief that in terms of poll worker training "less is more." The attempt to make poll workers conversant in every aspect of elections leads to confusion; confusion can lead to paralyzing of the poll worker who wishes not to make a mistake. This paralyzing of the poll worker can lead to delays in processing voters and introduced public and media concern regarding the reliability, accuracy and security of the election. Presiding Judge training and the ability to take a critical yet volatile group of citizens and make them election experts is impractical. SysTest Labs would also recommend that a Hot Line be available between the SOS and the county BOEs as a means of communication and an adjunct to training issues.

3.2.21.2 Second Chance Voting

Variations in voter protection over-rides on optical scan systems were observed in precinct optical scan counties. The over-ride function is used when the voter chooses to ignore the second chance voting warnings provided by the system. In some cases, the voters' ballots were placed in an emergency bin to be processed at the end of the day by the poll workers when the voter was no longer present. The second chance voting features of the voting systems are an important protection for the voter (and election officials) and over-riding the over vote protections should be done by the voter personally.

3.2.21.3 Vote Centers

Almost all counties assign a set of precincts to a common polling location for accessibility reasons when needed. When such assignments are made, many counties consider the location to be a "Vote Center" meaning that the electronic voting machines assigned to that polling location are programmed with ballots for all the precincts assigned to that location. Voters can then vote the correct ballot on any machine at that location. We concur that the practice is an efficient use of voting machines and resources and encourage it. However, the practice creates several potential risks that current practices do not address:

1. When devices used to encode voter cards or other devices used to activate the voters ballot at a given vote center use common codes, there is no automated means to prevent poll workers from using an encoder from another precinct and issuing the incorrect ballot. While procedures, visual cues and lanyards provide some protection in mitigating the risk, the risk can be eliminated entirely by using precinct unique codes within a vote center.
2. The efficiencies of having identical machines at a vote center and their utility in reducing or eliminating voter wait time and lines is undermined by the practice of assigning machines to each Presiding Judge for each precinct rather than to a single person for the vote center. The practice inevitably creates a false territoriality resulting in the machines being setup and employed to optimize voting at the precinct rather than at the vote center.
3. When machines are deployed in a vote center design, the unit of analysis for reconciling the ballots cast and the number of voters who voted shifts from the traditional precinct level, where voters are signed in, to the vote center. To effectively reconcile ballots to voters on election night, the voters must be aggregated and compared to the sum of ballots cast on all the machines. This reconciliation has either been eliminated due to the shift in levels of analysis or has been perpetuated at the precinct level where the reconciliation will never balance if the machines are employed optimally. The cognitive dissonance caused by the inability to reconcile meaningfully at the precinct level creates and reinforces the territoriality described above.

3.2.21.4 Issuing Provisional Ballots

Regarding paper provisional voting requirements, we explored proposed procedures for issuing provisional ballots while handling the flow of voters and line management. Few jurisdictions appear to have formulated plans to facilitate the process. Long lines and delays in voting resulting from provisional voters will only exacerbate concerns of disenfranchisement and machine malfunctions and pose a risk to voter confidence. This risk can be mitigated by the development of procedures that identify provisional voters early in the process and take them aside for processing and thereby not creating delays or bottlenecks for regular voters. An area which once enhanced policies, procedures and processes are developed should be thoroughly explained in detailed and focused poll worker training.

3.2.21.5 End of Day

With the exception of ballot/voter reconciliation procedures discussed above, end of day procedures generally provide adequate controls and security. It was noted that a number of counties co-mingle unused paper ballots and used paper ballots in the return container with no separate packaging or means of segregating one group from another as discussed previously.

3.2.21.6 Two Person Rule

An apparent inconsistency in the statutes regarding the two-person requirement for the custody of voted ballots and election material surfaced in every county. To wit, on election night ballots are returned to the BOE or designated drop stations by a single person, the Presiding Judge. Once the ballots are in the custody of BOE staff the two person rule is employed. Arguably, there is greater risk of tampering when the ballots are in the custody of a single person.

3.2.22 Reconciliation/Canvassing

Several new legal and operational requirements have changed the process of canvassing, auditing and reconciling unofficial election results in Ohio over the last few years. Changes in voting technology has resulted in most counties having multiple voting systems, one paper based (absentee) and one electronic (polls) or one central count (absentee) and one precinct count (polls). The volume of absentee ballots has increased dramatically due to new laws and the percentage processed after election night has increased. Finally, the requirement for provisional ballots has added additional processing steps and has required ballots to be counted after election night. The result is that there are new timelines and categories of ballots to be reconciled.

We observed counties employing traditional punch card, paper ballot and single voting system assumptions and techniques for canvassing election returns, modifying processes slightly to accommodate voting changes. These processes are adequate for canvassing paper ballots cast at the polls but do not always adequately audit electronic voting when vote centers are employed. Absentee ballots are not audited as rigorously as poll ballots and sometimes are not reconciled at all. A lack of understanding of auditing principles or big picture perspective on the objectives of the canvassing process have led to well-intended but fuzzy, partial and often inadequate post election checks and balances which are compounded by a lack of written documentation.

3.2.22.1 Qualification of Provisional Ballots

Provisional ballots are generally processed right after Election Day so they can be qualified and tabulated as soon as possible. We noted that in some cases, the checks for double voting at the polls were weak or non-existent and were manual processes whereas checks of double voting with absentees were thorough and automated. Provisional ballots are reconciled as individual transactions and we observed no aggregation and reconciliation at a precinct level. Some counties reported a practice in tallying and reporting provisional ballots that could compromise the secrecy of a voter's ballot; specifically, provisional ballots were tallied and reported in a unique category that would make it easy to determine how a voter voted in low turnout elections. It appeared that the basis of this practice might be a misinterpretation of the reporting of provisional voter statistics. If the practice is a result of a state requirement to report the results of provisional ballots separately, the policy should be revisited to protect the rights of voters.

3.2.22.2 Canvass Discrepancies

Most jurisdictions had practices in place to research and resolve discrepancies noted during the canvass however they were not formalized in written procedures. No county interviewed had a process in place to track, document and report resolved and unresolved issues resulting from the canvass process to the public and in many cases even to the Board. For purposes of transparency and confidence, we feel that the inevitable discrepancies that occur in every election should be documented. Such documentation would describe the nature of the discrepancy, what research was conducted to determine when, where, why and how it occurred, what corrective actions were taken, the impact of an unresolved discrepancy and actions to prevent similar discrepancies in the future. The documentation would be presented to the Board in a public meeting and would be part of the public record.

3.2.23 Risk Analysis Matrix

Table 12 is a detailed list of the risks identified in the Election Process and Operations Control Risk assessment activity.

Table 12 EPOC Probability and Risk of Unmitigated Vulnerabilities

ID	Unmitigated (UM) Probability Level	UM Failure Impact Level	UM Risk Assessment	Risk
EOIC-1	B	3	Yellow	Local procedures for security, access controls and election procedures generally are either incomplete or not adequately documented in writing.
EOIC-2	A	1	Red	BOE facilities provide inadequate physical security and access controls for voting machines, paper ballots and other sensitive and high dollar value items.
EOIC-3	C	2	Yellow	Partisan hiring practices result in less qualified staff in key positions and inhibit or prevent the conduct of background checks of BOE "insiders". The full scope of common public

ID	Unmitigated (UM) Probability Level	UM Failure Impact Level	UM Risk Assessment	Risk
				sector management practices such as performance evaluations; performance counseling, discipline and termination are unable to be effectively performed.
EOIC-4	D	2	Yellow	Voter Registration systems and voting system election management systems do not exchange common data resulting in multiple databases and parallel data management.
EOIC-5	D	1	Red	Software and firmware version controls, practices and documentation, at both the state and county level, do not protect against the introduction of unauthorized versions.
EOIC-6	A	2	Red	Existing statutory timelines and recent practices for certification of the contents of ballots to BOE create a critical constraint for all downstream election tasks resulting in quality control shortcuts and the potential introduction of unnecessary errors due to confusion and haste.
EOIC-7	B	2	Red	Logic and Accuracy testing is not effectively conducted to identify errors and verify the accuracy of individual machines, absentee ballots and the system as a whole.
EOIC-8	C	3	Yellow	The handling, counting and reconciling of absentee ballots is inconsistent with current volumes, reflects inconsistent interpretation of statute and decision on disqualification are inconsistent between counties.
EOIC-9	C	3	Yellow	Practices for sealing and securing voting equipment during transport and while out of the direct control of the BOE while thoughtful, systematically fail to provide an adequate means for detecting and quarantining of equipment that may have been tampered with.
EOIC-10	A	2	Red	Practices for Election Day operations are inconsistent and can create a level of confusion on both the voters part and PJ; while the use of voter centers with multiple precincts is employed the use of encoders by a respective PJ can result in the wrong ballot being issued; territorial issues can arise resulting in less than optimum use of voting machines. Additionally various methods for reconciling vote center results are not confusing and can result in erroneous

ID	Unmitigated (UM) Probability Level	UM Failure Impact Level	UM Risk Assessment	Risk
			🟥	reporting.
EOIC-11	A	2	Red	Practices for reconciliation / canvassing are predicated on traditional punch card, paper ballot and single voting system assumptions which are adequate for paper ballots but may be adequate for election voting particularly when vote centers are utilized; this situation can lead to partial and inadequate post-election checks, documenting of discrepancies and balances calling into question the accuracy of the results.

3.2.24 Countermeasures and Mitigation Analysis

Table 13 analyzes the impact of SysTest Labs proposed countermeasures and mitigation for the vulnerabilities identified and discussed in Table 12 as well as for potential vulnerabilities that have been proposed by other studies. These additional vulnerabilities are presented, in general terms and without attribution to a specific voting system technology. Please note that the ID number in Table 13 relates to the Risk identified in Table 12 EPOC Probability and Risk of Unmitigated Vulnerabilities.

Table 13 EPOC Proposed Countermeasures and Mitigation

ID	Mitigation	Threat Target(s)	Vulnerabilities	Deter	Delay	Detect	Deny
EOIC-1	An outline and standards for local procedures covering all election operations should be developed at the state level. Standards should also address inclusion of standardized, efficient and effective workflows for each voting technology and/or voting system.	II, III	Omission of important steps or practices Inconsistent procedures from one election to the next "Silo mentality" among staff Inadequate staff and poll worker training "Knowledge is power" gambits Lack of continuity when re-organization or staff turnover occurs Reliance on the personal judgment and decisions of Directors and staff	X		X	X
EOIC-1	Counties should be required to develop resulting written procedures which should be reviewed and approved by peers and/or the Secretary of State.	II	Incomplete, inadequate or inconsistent procedures Inefficient and ineffective procedures Improper priorities Improper use of resources	X	X	X	X

ID	Mitigation	Threat Target(s)	Vulnerabilities	Deter	Delay	Detect	Deny
EOIC-1	Periodic audits should be conducted to ensure counties comply with the procedures and that the procedures are updated to reflect changes.	II	Non compliance with procedures and policies Outdated or inaccurate policies Inefficient and ineffective procedures Improper priorities Improper use of resources				
EOIC-2	Conduct Physical Security and Crime Prevention assessment of facilities and implement recommendations	I, II, III	Inadequate facilities Misuse of space Unauthorized access Commingling of sensitive and non-sensitive materials and equipment Sharing of storage facilities with other County agencies	X	X	X	
EOIC-2	Install electronic lock system	I, II, III	Use of two-key locks to gain entry to sensitive areas Unauthorized access to sensitive, items and equipment	X	X	X	
EOIC-2	Employee and visitor badge and pass system	I, II, III	Unauthorized access to sensitive areas, items and equipment	X	X	X	
EOIC-2	Install Intrusion Detection System (IDS)	I, II, III	Building, offices and secure areas can be accessed when unoccupied. Unauthorized access to voting machines when facility is unoccupied Unauthorized access to EMS servers when facility is unoccupied Unauthorized access to unvoted ballots	X	X	X	

ID	Mitigation	Threat Target(s)	Vulnerabilities	Deter	Delay	Detect	Deny
			when facility is unoccupied Unauthorized access to voted absentee ballots when facility is unoccupied Unauthorized access to other sensitive items and equipment when facility is unoccupied Sabotage of critical or sensitive equipment Theft of ballots, sensitive items and high dollar value items Commingling of sensitive and non-sensitive materials and equipment				
EOIC-2	Install Video Surveillance System	I, III	Tampering with voting machines Modifying voting machine hardware Modifying EMS configuration Reprogramming voting machines Reprogramming EMS Changing EMS database Defeating/compromising security measures Altering vote totals in EMS tabulation/tally modules Tampering with voted absentee ballots Tampering with un-voted paper ballots Sabotage of critical or sensitive equipment Theft of ballots, sensitive items and high dollar value items	X	X	X	
EOIC-3	Standardized job descriptions, merit based hiring/firing practices, minimum qualifications	II	Unqualified staff in key positions	X	X	X	

ID	Mitigation	Threat Target(s)	Vulnerabilities	Deter	Delay	Detect	Deny
			Lack of personal accountability Ineffective management Ineffective organizational structures				
EOIC-3	Background checks for permanent and sensitive temporary positions	II, III	Employees with questionable or criminal background Staff susceptible to corruption or unethical behavior	X	X	X	
EOIC-3	State sponsored or mandated on-going professional training program and opportunities	II	Well intentioned but untrained staff Untrained management	X	X	X	
EOIC-4	Require vendors to create and/or automate data interfaces with support election management systems (and require counties to use them)	II	Multiple manual data entry of precinct, district and candidate information from VR system to ballot layout and EMS applications Parallel maintenance of similar data bases Lack of data synchronization Increased number of points of failure/error Multiple proofing QC events and process for same data Time delays in critical time sensitive processes	X	X	X	
EOIC-5	Standardized and centralized software and firmware installation and version control protocol	I, II, III	Use of uncertified software Mismatch between certified and installed software Incomplete or partial installation of SW/FW Unknown source or version of SW/FW Non conforming configurations	X	X	X	

ID	Mitigation	Threat Target(s)	Vulnerabilities	Deter	Delay	Detect	Deny
EOIC-5	Standardized record keeping of current software and firmware versions		Lack of SW/FW chain of custody Inability to know when and by whom SW/FW installed Unknown current versions	X	X	X	X
EOIC-6	Filing requirement statutes, regulations and directives should be formally reviewed and revised with an emphasis on bringing them in line with current technologies and their new constraints and timelines. Specific area to examine include: timelines for inclusion of candidates, offices, measures and local options on the ballot.		Incorrect ballot contents Truncated proofing and QC Late ballot printing Over committed ballot printers Improperly printed ballots Late or incomplete database setup Incomplete or inaccurate programming of voting machines Truncated L&A testing and QC of voting equipment Version control and data synchronization issues	X	X	X	
EOIC-7	Standardize LAT Testing criteria and protocols at a state level to include a complete end to end battery of tests of individual machines, central count systems, server based accumulation and reporting systems and internet reporting applications.	II, III	Incomplete LAT testing Critical items not tested Full voting machine functionality not tested Missing Contests/Candidates/Precincts Inconsistent testing of machines within a jurisdiction Inconsistent testing of machines between jurisdictions Conflicts between electronic and paper based ballots Vote accumulation and integration conflicts between electronic and optical	X		X	X

ID	Mitigation	Threat Target(s)	Vulnerabilities	Deter	Delay	Detect	Deny
			systems Election night tabulation delays Election night reporting delays Improper voting machine exception handing functions (over vote, under vote, write-in) Introduction of rogue programming Incorrect date and time settings Calibration and sensitivity problems				
EOIC-7	Implement a "Parallel Testing" program by the state to test a randomly selected sample of voting machines from a representative sample of jurisdictions on election day by casting a test script, videographing the voting process and reconciling the reported results against the predetermined script.	III	Introduction of rogue programming into voting machines and EMS Trojans and other malware in voting machines and EMS	X	X	X	X
EOIC-8	Absentee voting statutes, regulations and directives should be formally reviewed and revised with an emphasis on bringing them in line with current technologies and voting practices. Specific areas to examine include: absentee ballot processing timelines, accounting procedures, security requirements and disqualifying criteria.	II	Inadequate capacity to process volume of ballots on current timelines Incomplete or inaccurate absentee vote totals on election day Lack of accountability and audit trails of voted ballots Delay in reporting election day results Voter privacy and secret ballot compromised by stub number practices Eligible ballots disqualified by absence of stub Inconsistent qualification/disqualification criteria between counties Inconsistent "second chance voting" and exception handling	X	X	X	

ID	Mitigation	Threat Target(s)	Vulnerabilities	Deter	Delay	Detect	Deny
			Inconsistent application of voter intent standards and ballot duplication practices				
EOIC-9	Establish a standard of inventory controls that identifies sensitive items requiring on-going serial number accountability, the frequency of inventories and actions for missing inventory.	I, II, III	Loss of sensitive items Loss of control of sensitive items Theft, loss or loss of control of voting machines and equipment.	X	X	X	X
EOIC-9	Develop practical, reasonable standard tamper detection practices and security standards for equipment and supplies during transport and for storage when out of the direct control of BOE staff to include guidelines for the use of serial numbers.	I, II, III	Loss or theft of ballots and voting material. Tampering with voting equipment Unauthorized access to sensitive components of voting machines Inconsistent practices Meaningless and counterproductive practices to secure voting equipment Machines, encoders and cards issued to a single person or stored together	X	X	X	
EOIC-9	Establish standards for contractors that deliver or store voting equipment that include bonding, insurance, background checks and election worker oaths.	I, III	Loss or theft of ballots and voting material. Tampering with voting equipment Unauthorized access to sensitive components of voting machines	X	X	X	
EOIC-10	Develop Election Officer training guidelines, programs and workshops that prioritize training topics, test comprehension, reduce class time and lead to increased retention of qualified workers	I, II	Too much material covered Unrealistic expectations Training effectiveness and comprehension not known Loss of attention and interest during long training sessions Qualified and experienced workers not retained	X	X	X	X

ID	Mitigation	Threat Target(s)	Vulnerabilities	Deter	Delay	Detect	Deny
EOIC-10	Develop standard criteria for handling second chance voting on precinct count optical scan systems.	I, II	Voter privacy violated Secret ballot compromised Ballots mishandled or uncounted Second chance opportunities unequally applied	X	X	X	X
EOIC-10	Formally recognize the practice of Vote Centers in statute and directive and develop standards and processes that leverage their advantages of accessibility, convenience, efficiency and control.	II	Voters voting wrong ballot Loss of ballot accountability Precinct territoriality Potential cost savings and efficiencies not realized Misprocessing provisional voters	X	X	X	X
EOIC-10	Develop alternative practices for issuing and managing paper provisional ballots on election day.	I, II	Long lines for all voters Unnecessary delays for all voters Ballots mishandled Ballots inadvertently tallied Poll worker confusion	X	X	X	X
EOIC-10	Develop or clarify voted paper ballot security and transportation requirements.	I, II	Voted and non voted ballots co-mingled Loss of accountability of voted ballots Inconsistent levels of security for ballots	X	X	X	X
EOIC-11	Establish standards and procedures for canvassing, auditing and reconciling election returns that consider multiple voting systems, types of technologies and types of ballots.	II	Eligible ballots not counted and reported Ballots counted multiple times Ballots miscounted Ballots misread Ballots counted in incorrect precincts Absentee ballots not accounted for or reconciled	X		X	X

ID	Mitigation	Threat Target(s)	Vulnerabilities	Deter	Delay	Detect	Deny
			Operator errors Inaccurate compilation of paper and electronic results				
EOIC-11	Establish or clarify requirements and procedures for processing provisional ballots	II	Undetected double voting Voter privacy Secret ballot compromised	X		X	X
EOIC-11	Establish a framework or template with corresponding procedures for documenting discrepancies and efforts made to resolve them to ensure comprehensive and standardized practices at the county level.	II	Lack of transparency Public mistrust Non disclosure of known issues Inadequate explanation of corrective actions	X		X	X

3.2.25 Conclusions

The conclusion of the Election Operations & Internal Control Assessment Team is that the most significant vulnerabilities and risks to elections in Ohio are not directly a result of weaknesses voting hardware, software or firmware. In fact, to our surprise, the vulnerabilities and risks we observed and have addressed in this report are independent of voting system, class of technology (electronic or optical) or voting system vendor. We recognize that these observations are contrary to the current furor and common wisdom that continues to scapegoat voting technology as the source of ambiguity and uncertainty in the integrity of elections.

Nonetheless, we have concluded that the greatest risks to voting are a result of inconsistent practices, the absence of adequate guidelines, standards and procedures as well as the perpetuation of outdated assumptions and practices. All of these are exacerbated the rapid pace of change in public expectations, evolving legal requirements, the pace of technological change and the peculiar partisan overlay of the election administration process in Ohio.

We recognize that our analysis and recommendations imply greater centralization and less autonomy for local election officials and will be received by them with some skepticism and by some as threatening. We also recognize that our analysis and recommendations place greater responsibility and accountability on the Secretary of State’s office for which it is probably inadequately resourced both in terms of positions and technical expertise. And we recognize that this report is based upon different assumptions from other software and hardware focused portions of the EVEREST project and other voting system studies and therefore it is no surprise that this report comes to different conclusions as to the nature of the issues and their resolution. We feel these observations and recommendations speak for themselves and require no further justification or appeal to the experience or academic credentials of the team.

It is clear to us that the vulnerabilities and risks identified in this report are independent of any voting system specific risks that might also exist. Independent of voting systems actions and reforms resulting from the EVEREST project (such as decertification, system redesign, technical risk mitigation measures, etc), if the operational status quo is maintained the issues, risks and challenges identified in this report and observed in past elections will be largely, if not completely, unaffected.

3.3 Configuration Management

The SysTest Labs Risk Assessment Team performed a Physical Configuration Audit and reviewed supporting documentation for a voting system installed at the State of Ohio Computing Center in Columbus, Ohio. The purpose of the audit was to verify that the configuration of a sample system, as defined by the hardware, firmware and software revision levels, was on the State of Ohio list of certified systems.

In addition, the SysTest Labs team assessed the processes and procedures used by the State of Ohio to manage the equipment configuration in the field. Of particular interest were the configuration management practices for ensuring that the equipment was at the proper certified level and how updates and upgrades are handled.

SysTest Labs also conducted a review of the Logic and Accuracy (L&A) procedures in use by the counties. We particularly looked for consistency across the State of Ohio certified and deployed vendors' equipment and if the procedures included steps for the verification of the hardware, firmware and software versions in use by the counties.

3.3.1 Premier Election Systems Specifics

Premier Election Systems has certified certain thermal printer paper, ballot stock, and PCMCIA memory devices to work with their system. The use of materials other than those specified can result in significant problems.

3.3.2 ES&S Specifics

ES&S has specified certain compact flash storage devices, ballot stock, and thermal printer paper to be used for elections. The use of materials other than those specified can result in significant problems.

3.3.3 Hart InterCivic Specifics

Hart has specified certain PCMCIA memory devices, thermal printer paper, and ballot paper stock and ballot fonts to be used for elections. The use of materials other than those specified can result in significant problems.

3.3.4 Conclusions

A physical configuration audit of sample Ohio certified voting systems from each of the three deployed system vendors and assessment of the configuration management procedures identified risks to be addressed. The most significant issue is ensuring that information is available so that personnel can make the correct decision.

A summary of the risks from a configuration management perspective are as follows:

1. The use of materials that have not been certified by the manufacturers could create significant risks.
2. We researched the ability to provide a procedure for verification that the firmware/software installed in a unit is equivalent to the certified version and has not been changed during an election. We found that any procedure to perform this operation before and after an election would be impractical for current ES&S and Premier systems. They require the disassembly of the unit, physical extraction of the memory device and utilization of

specialized equipment to read the data. Hart InterCivic is currently the only manufacturer who has implemented a software routine that uses hash codes for verification of their firmware/software. This capability needs to be provided by the other manufacturers as soon as possible.

3. Dissemination of information to the counties including L&A procedures is not consistent.
4. The revision levels of all systems in the counties are unknown and not tracked.

3.3.5 Configuration Management Risk Assessment Result Tables

Table 14 Hart InterCivic Risks/Mitigation

Hart InterCivic					
ID	**Probability of Occurrence**	**System Impact Level**	**Risk Assessment**	**Risk**	**Mitigating Factors**
CM-HRT-1	**B**	**3**	**YELLOW**	The installed and as-built configuration (defined by hardware, firmware and software revision levels) of Hart InterCivic voting system equipment in the counties throughout the State of Ohio is unknown.	Provide a means for creating and maintaining a centralized database of the field inventory by county containing manufacturer, model, serial number and revision level information. The database shall be readily accessible by county BOE personnel for verifying the revision levels of their equipment.
CM-HRT-2	**B**	**3**	**YELLOW**	Logic and Accuracy (L&A) procedures are not consistent throughout the counties using the Hart InterCivic's voting system or have not been provided to the county BOEs by the SOS organization as required by the 2006 directive.	Provide a centralized source for dissemination of information (L&A procedures, hardware/software compatibility information and user documentation).
CM-HRT-3	**B**	**2**	**RED**	Hart InterCivic has certified certain consumables and storage devices for use with their voting system. There are uncertified forms of these materials readily available in the open market. Safeguards cannot be built into the system to ensure that the PCMCIA storage cards (MBB), thermal printer paper, ballot paper and ballot fonts are the type certified for use. The use of uncertified materials can result in significant failures during an election.	Provide a centralized source of information accessible by county BOE personnel that clearly specifies any consumables or storage devices that are to be used with the system. Clearly communicate to the BOE personnel that using something other than the specified materials may result in failures during an election.

Hart InterCivic					
ID	**Probability of Occurrence**	**System Impact Level**	**Risk Assessment**	**Risk**	**Mitigating Factors**
CM-HRT-4	**D**	**2**	**YELLOW**	The Hart InterCivic SERVO software system, provided for testing and analysis by SysTest Labs as part of the Ohio risk assessment was missing a file necessary for verifying the hash codes of the operating software. This indicates that the software installed in voting system equipment in the counties may not be equivalent to the certified version.	The SOS organization shall produce and distribute media containing a complete binary image of the certified version of software to be installed on a voting machine. The binary image can be produced using Norton Ghost™ or a similar imaging utility. • Verification of the loaded software shall be accomplished by using the Hart InterCivic utility to verify authenticity as a step in the L&A procedure. • If the loaded software is found to not be equivalent to the certified version, the image must be reloaded from the supplied media.
CM-HRT-5	**D**	**2**	**YELLOW**	There is no evidence to indicate that the county BOE personnel utilize the Hart InterCivic code verification procedure for ensuring that the firmware and/or software installed in the voting system equipment has not been compromised before or after an election.	1. Verify that the procedure that Hart InterCivic provides is disseminated to all counties that have Hart InterCivic equipment. 2. Educate the county BOE personnel on its use. 3. Invoke the procedure every time the equipment is prepared for use. 4. Document the results of the verification.

Table 15 ES&S Risks/Mitigation

ES&S					
ID	**Probability of Occurrence**	**System Impact Level**	**Risk Assessment**	**Risk**	**Mitigating Factors**
CM-ESS-1	**B**	**3**	**YELLOW**	The SysTest Labs risk assessment team encountered an iVotronic unit that had down level software installed. This indicates that the installed and as-built configuration (defined by hardware, firmware and software revision levels) of ES&S voting system equipment in the counties throughout the State of Ohio is unknown.	Provide a means for creating and maintaining a centralized database of the field inventory by county containing manufacturer, model, serial number and revision level information. The database shall be readily accessible by county BOE personnel for verifying the revision levels of their equipment.
CM-ESS-2	**B**	**3**	**YELLOW**	Logic and Accuracy (L&A) procedures are not consistent throughout the counties using ES&S's voting system or have not been provided to the county BOEs by the SOS organization as required by the 2006 directive.	Develop a centralized means for dissemination of information (L&A procedures, hardware/software compatibility information, user documentation, equipment inventory database).
CM-ESS-3	**B**	**2**	**RED**	ES&S has certified the use of compact flash memory devices with Athens 1 or 2 controllers and specific thermal printer paper for their voting systems. There are uncertified forms of these materials readily available in the open market. Safeguards cannot be built into the system to ensure that the compact flash storage cards and thermal printer paper are the type certified for use. The use of uncertified materials can result in significant failures during an election.	Provide a centralized source of information accessible by county BOE personnel that clearly specifies any consumables or storage devices that are to be used with the system. Clearly communicate to the BOE personnel that using something other than the specified materials may result in failures during an election.
CM-ESS-4	**D**	**2**	**YELLOW**	The ES&S election management software system, provided for testing and analysis by SysTest Labs as part of the Ohio risk assessment was missing files. This was an indicator that the software installed in other	The SOS organization shall produce and distribute media containing a complete binary image of the certified version of software to be installed on a voting machine. The binary image can be produced using Norton Ghost™ or a similar imaging utility.

ES&S					
ID	**Probability of Occurrence**	**System Impact Level**	**Risk Assessment**	**Risk**	**Mitigating Factors**
			🟨	voting system equipment in the counties may not be equivalent to the certified version	• Verification of the loaded software shall be accomplished by comparing a generated SHA-1 message digest with a message digest from the certified version to verify authenticity as a step in the L&A procedure. • If the loaded software is found to not be equivalent to the certified version, the image must be reloaded from the supplied media.
CM-ESS-5	**D**	**1**	**RED**	The SysTest Labs risk assessment team analyzed the ES&S system in an attempt to recommend a procedure that could be used to verify that the software and firmware loaded in a unit was equivalent to the certified version before and after an election. The results of the analysis concluded that the procedure would be impractical to perform on all units in the field. The firmware in the iVotronic voting machine that is part of the Unity voting system could be compromised and modified without detection. This conceivably can occur before, during or after an election.	The procedure for ensuring that the firmware in a machine is identical to the certified version for ES&S equipment requires disassembly of the unit, physical extraction of the non-volatile memory device and use of special equipment to read the binary data for comparison. This procedure, although possible, is very cumbersome and can only be performed by qualified personnel. The best solution to mitigate this risk is for the State of Ohio to require all manufacturers to implement an automated software routine that reads the binary data from the memory and generates a SHA-1 message digest for comparison with a message digest from the certified version. The SOS Office should make this part of their State certification requirements.

Table 16 Premier Risks/Mitigation

Premier					
ID	Probability of Occurrence	System Impact Level	Risk Assessment	Risk	Mitigating Factors
CM-PRM-1	B	3	YELLOW	The installed and as-built configuration (defined by hardware, firmware and software revision levels) of Premier voting system equipment in the counties throughout the State of Ohio is unknown.	Provide a means for creating and maintaining a database of the field inventory by county containing manufacturer, serial number, revision level, information. The database shall be readily accessible by county BOE personnel for verifying the revision levels of their equipment.
CM-PRM-2	B	3	YELLOW	Logic and Accuracy (L&A) procedures are not consistent throughout the counties using the Premier's voting system or have not been provided to the county BOEs by the SOS organization as required by the 2006 directive.	Develop a centralized means for dissemination of information (L&A procedures, hardware compatibility information and user documentation).
CM-PRM-3	B	2	RED	There are no safeguards to ensure that only certified consumables and PCMCIA storage card are used in a Premier voting system.	Provide a centralized source of information accessible by county BOE personnel that clearly specifies any consumables or storage devices that are to be used with the system. Clearly communicate to the BOE personnel that using something other than the specified materials may result in failures during an election.
CM-PRM-4	D	1	RED	The SysTest Labs risk assessment team analyzed the Premier system in an attempt to recommend a procedure that could be used to verify that the software and firmware loaded in a unit was equivalent to the certified version before and after an election. The results of the analysis concluded that the procedure would be impractical to perform on all units in the field.	The procedure for ensuring that the firmware in a machine is identical to the certified version for Premier equipment requires disassembly of the unit, physical extraction of the non-volatile memory device and use of special equipment to read the binary data for comparison. This procedure, although possible, is very cumbersome and can only be performed by qualified personnel. Premier has documented a procedure for performing this operation. The best solution to mitigate this risk is for the State of Ohio to require all manufacturers to implement an automated software routine that reads the binary data from the memory and generates a SHA-1 message digest for comparison with a message digest from the certified version. The SOS Office should make this part of their State certification requirements.

3.4 Performance Testing

As part of the Performance Test Plan, SysTest Labs' Risk Assessment Team created test cases intended not to pass or fail any component of the voting system, but to observe the result and any possible deficiencies in an election process. Testing will emphasize:

- Preparing for an election

  Considering the number of personnel and polling locations needed to conduct an election, creating an election and setting up the equipment can be very daunting. SysTest Labs created and set up an election in accordance with the vendor documentation that was supplied to SysTest Labs in order to observe if any risks can arise due to lack of appropriate documents.

- Accuracy and integrity of the Voting process

  As is with all elections, electronic or non-electronic, the accuracy of an election and the confidence of every vote being counted is of the utmost importance. SysTest Labs created its own election definition, in accordance with the EAC guidelines, voted on the DRE and Optical Scanner and observed if every vote accounted for in the final tally after consolidation. Also, the official results for the State of Ohio are the individual ballots printed on the DRE. Testing also includes VVPAT testing and the accuracy of the results tape from the DRE as well as the optical scanners. In addition Volume testing was conducted on each system and verified that votes will not be lost due to any memory leak.

- Accuracy of Audit logs

  In the event of any discrepancies to the election process, the Audit logs will need to be examined to resolve or investigate any issues. The Audit logs were examined to see if any risks exist due to the lack of logging specific events that were done on the DRE which would hamper the State of Ohio to re-create any voting day scenarios.

3.4.1 Premier Observations

The SysTest Labs' risk assessment team executed a voting system specific test plan to assess the usability and accuracy of version 1.18.24 of the GEMS Voting system as deployed within the State of Ohio. Tests of the devices used to record ballots cast including TSx direct record electronic (DRE) voting terminals, the AccuVote central count optical scanners, and the AccuVote precinct ballot optical scanners were included in the executed test plan.

The GEMS Voting System is a feature rich voting solution. The GEMS Voting System offers flexibility in election definition and ballot design capabilities.

The objective of SysTest's assessment was to identify potential risks to the integrity of the voting processes, including the accuracy of the vote tally process, as implemented by the GEMS Voting System as currently used within the State of Ohio. Testing was performed at the State of Ohio Computing Center (SOCC) in Columbus, Ohio on equipment supplied by the State of Ohio.

The testing process included examination of the GEMS Voting System's functionality related to defining an election, electronic and paper ballot configuration, installation of the election definition on the system's voting components, casting predetermined test ballots on the system's voting components, and collection, consolidation and reporting of the test ballots cast. Additionally, administrative and audit logging functionalities of the various system components were also examined.

Test cases included:

- Conducting an inventory of the provided GEMS Voting system components
- Physically setting up and configuring the GEMS Voting system components
- Creation of the election definition database
- Installing the election definition on all of the voting hardware
- Voting accuracy testing of all of the voting hardware
- Collecting and consolidating all of the cast ballots' votes
- Verifying entries to the Voter Verifiable Paper Audit Trail (VVPAT)
- Exercising administrative functionalities of the system components
- Capacity testing of the various GEMS Voting system media and memories
- Examining Audit Log entries made by the GEMS Voting software.

SysTest Labs also attempted to verify that the versions of the GEMS Voting System applications provided for testing were the same as the official versions deployed in the State of Ohio. SysTest Labs examined the directory tree structures and file sizes of the software loaded on the servers and compared these to expected results. The State, however, was unable to provide an official installation distribution against which to compare SysTest's findings.

3.4.1.1 Documentation

Although County staff may become experts in the voting system that does not imply a sufficient expertise required for installation of the system. Understanding that training is provided by the Premier on their voting system, User Manuals/Guides and other documentation will be needed to conduct an election such as: set-up system at the Central Count and Poll locations, create elections using vendors GEMS and consolidate votes for final tally. While testing at the Ohio Computing Center, SysTest Labs used this documentation as a reference to set-up & conduct an election and had documented any deficiencies and omitted information that was found to be pertinent information.

3.4.1.2 VVPAT – AccuVote TSx Printer

The VVPAT thermal paper can be easily installed backwards which would cause the TSx to try and print on the wrong side. The documentation does not address this issue and Poll Workers Guide recommends if no writing occurs, take the unit out of service. This could lead to unit being taken out of service when not needed. It should also be noted that VVPAT paper does have a finite shelf life.

Generally, VVPAT paper will remain human readable for a minimum of 10 years, if imaged to saturated density and stored under the following conditions:

- Temp less than 77 F.
- Relative humidity less than 70%
- Stored in a dark environment, avoiding natural or artificial light
- Avoiding contact with chemicals such as plasticizers, oils, solvents, water and adhesives.

3.4.1.3 Hardware System Set up

Documentation for the AccuVote OS – Central Count hardware configuration is located in the TDP and not in any of the Manuals. The TDP is not normally distributed to the counties and can delay setting up equipment. This documentation includes setting up the AccuVote OS to the Digiport Hub and the DigiPort connection to the Hub. Also, there was no documentation instructing how to connect the EMP, or Smart Card Reader.

3.4.1.4 DHCP Service

Premier has a ‘GEMS Server Configuration Guide’, which lists the services to be enabled and instructs that all other services should be disabled. After disabling the DHCP service, we were unable to download election definition onto the PCMCIA cards that are located inside the TSx devices. This method is used if a high volume of cards needs to be created. If a user follows these instructions, it can delay the process.

3.4.1.5 File and Registry Permissions

Because the Digital Guardian are now installed on GEMS server as a security measure, it did prevent us from accessing the ‘manage computer’ component to verify permissions outlined in Section 3.3.5 of the GEMS Server Configuration Guide. Some administrative files might not be accessible to certain users.

3.4.1.6 VVPAT – AccuVote TSx Printer functionality

The State of Ohio official results is the paper trail that was created by the VVPAT printer during the voting process. Therefore, it is of the utmost importance that the VVPAT is fully functional for the Voter and the Poll Worker.

3.4.1.7 Ballot Visibility

VVPAT did not list the entire ballot for the Voters Ballot Review on the VVPAT. The last line, which contained the Write-In on the ballot, was not visible during testing. This could lead to voter discontent. A re-calibration of the printer will need to be performed. Also, if a candidate has an unusually long name, the name will be cut off at 20 characters on the paper ballot even though it is fully visible on the screen. This might confuse the voter.

3.4.1.8 Printing Long Reports

When the Audit Log, Zero Tape or Results Report is printed, the printer's Take-Up does not always work correctly. The paper does sometimes 'bunch up' in the VVPAT casing. Also, the TSx does not give a message when the Audit Report is finished printing. This could cause the user to believe printing is not complete.

3.4.1.9 TSx Functionality

Although the TSx did function as described in the documentation, it was not consistent. Some functionality had to be repeated or adjusted.

3.4.1.10 Improper Message

When powering the TSx unit after an election has been loaded, TSx displays an "Install & Test Printer" message. A printer does not required to be installed but only tested. This could cause the user to believe the printer is defective.

3.4.1.11 Smart Cards

Smartcards are media devices that serve different functionality; either as a Voter Access Card, Supervisor Card, or Administrative Card. It was discovered during the testing process that the Smart Cards used on the TSx unit could become disabled. A supervisor card unexpectedly became disabled and was not re-programmable.

3.4.1.12 PCMCIA Cards

When the PCMCIA cards were loaded into the TSx, it was not detected. Had to remove and re-insert the card. This could cause the user to believe card is defective.

3.4.1.13 AccuVote OS (Paper Ballot Scanners) - Changing Ballot Style

Conducting an election involved both the DRE and the Scanners. An issue did arise which could cause printed paper ballots to fail the L&A process. SysTest Labs had created its own election definition for testing; before the Ballot Style was exported to PDF for printing purposes. The ballot style was changed before re-generating art work. This caused the AccuVote OS Precinct Count configuration to ignore 2 races on the paper ballot. This would fail at the L&A process

3.4.1.14 Security

The same universal key can be used for all TSx units. This is a security issue because keys are not stored securely and PCMCIA can be removed. This would cause the VVPAT paper trail to be manually counted to acquire vote tally.

In addition, when an unauthorized card was inserted in the Smart Card slot, event was not recorded in the Audit Log. Counties will not be able to confirm if voter attempted to tamper with the TSx unit.

3.4.1.15 Volume Testing

Accuracy is tested during qualification, but not when the capacity of the system is stretched to its limit. Therefore capacity testing was conducted on the system.

3.4.1.15.1 Storage Devices

Capacity testing was also conducted on the storage devices (PCMCIA Cards & AccuVote OS Cards) during the download. A proper error message was given to user when a download of an election definition, that exceeded the storage devices memory capacity, was attempted.

3.4.1.15.2 AccuVote OS Load Test

SysTest Labs manually scanned over 10,000 ballots to observe if any votes will be lost. A Test Deck provided by Dayton Legal Blank was used. A test deck of 98 ballots was scanned 103 times. It was discovered that the Access Database GEMS uses to store votes are stored at a precinct level. Therefore a ballot image of each paper ballot is not kept, rather a numeric tally for each candidate at a precinct level.

3.4.1.15.3 TSx (DRE) Capacity Testing

The TSx that premier uses for elections use a 128 MB PCMCIA card (PC Card). The card needs to be loaded with the election definition before a user can begin voting on them. The size of the election definition can vary from one election to another especially if audio files are loaded for the hearing impaired. Testing was conducted to observe the behavior of the TSx unit when the PCMCIA card reaches its 128MB load capacity. It was observed that exceeding the capacity on the PCMCIA cards while voting on the TSx results in the PCMCIA cards being purged to make more room by deleting files on the card. Files that were purged and lost were files containing the votes. Although the EMP does not allow for a download of a 128MB PCMCIA card unless the result of a download allows for 26MB of free space, the PCMCIA card can exceed its memory capacity during a high volume of voting. The ballots on the VVPAT paper trail will need to be manually counted which is a very tedious and laborious task.

Table 17 Premier Performance Test Risk Assessment Table of Results

ID	Probability of Occurrence	System Impact Level	Risk Assessment	Risk	Mitigating Factors
PERF-PRM-1	**B**	**3**	**Yellow**	Documentation for the AccuVote OS – Central Count hardware configuration is located in the TDP and not in any of the Manuals. TDP is not handed out to counties and can delay setting up equipment. This documentation includes setting up the AccuVote OS to the Digiport Hub and the Digiport connection to the Hub.	Update documentation for the AccuVote-OS Central Count
PERF-PRM-2	**C**	**1**	**Red**	AccuVote-TSx **erases** vote data on the PCMCIA card during the voting process when memory capacity is exceeded on PCMCIA card.	Limit the number of voters that can vote on a TSx. Determine the amount of free space on the card and how much memory each cast ballot will consume. Calculate the number of voters allowed on each TSx. Or when failure occurs, will need to hand
PERF-PRM-3	**D**	**4**	**Green**	AccuVote OS-Central Count was scanning ballots but not reading the votes after a configuration change in GEMS. Needed to Power off/on the Digiport hub and AccuVote OS. Could delay L&A.	Document the risk for the GEMS user/administrator.
PERF-PRM-4	**C**	**3**	**Yellow**	The Windows Services (DHCP Server Service), on the GEMS Server, weren't configured according to the GEMS documentation. Could result with performance not equating the one	Server administrator will perform full configuration check on server before election process.

ID	Probability of Occurrence	System Impact Level	Risk Assessment	Risk	Mitigating Factors
				during qualification.	
PERF-PRM-5	**C**	**3**	**Yellow**	The VVPAT thermal paper can be easily installed backwards which would cause the TSx to try and print on the wrong side. The documentation does not address this issue and Poll Workers Guide recommends if no writing occurs, take the unit out of service. Could lead to unit being taken out of service when not needed.	Supplemental documentation and/or training need to be provided to the poll workers.
PERF-PRM-6	**C**	**3**	**Yellow**	VVPAT does not list the last entire ballot for the Voters printer tape review. The last line which contained the Write-In on the ballot was not visible during testing. This could lead to voter discontent.	Conduct an L&A on the VVPAT prior to opening the polls.
PERF-PRM-7	**C**	**4**	**Green**	Documentation instructs the poll worker 'To cancel a ballot, touch the pager number on the screen for 10 seconds'. But actual time was closer to 15 seconds. This could lead the poll worker to believe that the cancel option is not available.	Supplemental documentation and/or training need to be provided to the poll workers to press screen for at least 20 seconds.
PERF-PRM-8	**D**	**4**	**Green**	Voted name on VVPAT print out was cut off. Ex: Selected "Thomas Devine & Sharon Beck", but VVPAT writes "Thomas Devine & Shar"	Conduct an L&A on the VVPAT prior to opening the polls. If problem occurs, re-calibrate VVPAT.
PERF-PRM-9	**C**	**4**	**Green**	When printing the	Supplemental

ID	Probability of Occurrence	System Impact Level	Risk Assessment	Risk	Mitigating Factors
				Audit Log, TSx does not give message that printing is complete. This could cause the poll worker to believe that the VVPAT is not functioning properly. This could cause a delay in reporting results.	documentation and/or training need to be provided to the poll workers.
PERF-PRM-10	**D**	**4**	**Green**	During the printing of results and audit logs, VVPAT take-up did not always work properly and tape did ‘bunch up’ which caused subsequent printing to print on 1 line. Could cause a delay in reporting results.	Additional time needs to be allotted in case problem occurs.
PERF-PRM-11	**D**	**3**	**Yellow**	TSx did not initially recognize the PCMCIA Card with loaded election. Needed to re-insert card to be recognized. This could lead poll worker to believe card is defective and not be used.	Supplemental documentation and/or training need to be provided to the poll workers.
PERF-PRM-12	**C**	**4**	**Green**	When re-starting the TSx after it was powered down, an “Install & Test Printer” message appeared. Only a test needs to be conducted. This could lead the poll worker needlessly re-placing the paper tape.	Supplemental documentation and/or training need to be provided to the poll workers.
PERF-PRM-13	**D**	**3**	**Green**	One Supervisor Card out of four became disabled. This could lead to delays in the polling station.	Additional Cards need to be supplied.
PERF-PRM-14	**D**	**2**	**Yellow**	Changed ballot style of the paper ballots in	A complete L&A needs to be

ID	Probability of Occurrence	System Impact Level	Risk Assessment	Risk	Mitigating Factors
			🟨	GEMS at the last minute. Did cause AccuVote OS (1.96.6) to ignore one race.	conducted on absentee ballots with every single race being voted.
PERF-PRM-15	**D**	**4**	**Green**	The GEMS Server Configuration Guide, Sect 3.3.2 lists the 'services other than the following should be disabled'. Which indicates DHCP should be disabled. DHCP needs to be enabled if user wants to download/upload directly to the TSx.	Supplemental documentation and/or training need to be provided to the person configuring the server.
PERF-PRM-16	**C**	**4**	**Green**	The GEMS Server Configuration Guide, Sect 3.3.5 lists the File and Registry permissions. But unable to access the 'manage computer' component to verify permissions because Digital Guardian did not allow access. Some administrative files might not be accessible to certain users.	Access permissions needed to be set for administrator only. Issue can be addressed through Digital Guardian settings. Password must be setup for qualified/trained BOE personnel. Password security levels process and procedure must be established and adhered to and strictly enforced.
PERF-PRM-17	**D**	**4**	**Green**	There is no documentation instructing how to connect the EMP.	Update documentation for the Accuvote-OS Central Count or require basic network connectivity knowledge for person setting up the Central Count workstation.
PERF-PRM-18	**D**	**4**	**Green**	There is no documentation instructing how to connect the ST-100 SmartCard reader to	Update documentation for the AccuVote-OS Central Count or require basic network connectivity

ID	Probability of Occurrence	System Impact Level	Risk Assessment	Risk	Mitigating Factors
				GEMS Server COM1	knowledge for person setting up the Central Count workstation.
PERF-PRM-19	**D**	**4**	**Green**	When a non-smartcard is inserted in the smartcard slot during an election, it is not recorded in the audit log. Though it did reject the unknown card, this will hamper any investigation of possible tampering.	Provide added personnel at the polling station.
PERF-PRM-20	**D**	**4**	**Green**	While an election is loaded and the second PCMCIA card slot is open, a PCMICA card was inserted and it was not recorded in the audit log. Though it was ignored by the TSx, this will hamper any investigation of possible tampering.	Provide added personnel at the polling station.
PERF-PRM-21	**D**	**3**	**Green**	The same universal key is used for all TSxs to open cover of PCMCIA card slot. Someone i.e. Old employee, can open the TSx and take the PCMCIA card. This will disable TSx until another card can be inserted and delay reporting results since results won't be able to be uploaded and will have to be counted from the VVPAT tape.	Provide added personnel at the polling station.
PERF-PRM-22	**C**	**4**	**Green**	Premier does not have a separate Early Voting mode. Early Voting is handled by powering down the TSx for the day. GEMS generated results will not indicate any tally/metrics for	If Early Voting tally is desired, will need to count ballots directly from the VVPAT paper trail.

ID	Probability of Occurrence	System Impact Level	Risk Assessment	Risk	Mitigating Factors
			🟩	Early Voting.	

3.4.2 ES&S

The SysTest Labs' risk assessment team executed a voting system specific test plan to assess the usability and accuracy of version 3.0.1.1 of the ES&S Unity Voting System as deployed within the State of Ohio. Tests of the devices used to record ballots cast including iVotronic direct record electronic (DRE) voting terminals, M100 precinct ballot optical scanners, and M650 central count ballot optical scanners were included in the executed test plan.

The ES&S Unity Voting System is a feature rich voting solution. The Unity Voting System offers incomparable flexibility in election definition and ballot design capabilities. The Unity Voting System is used in 38 of Ohio's 88 counties.

The objective of SysTest's assessment was to identify potential risks to the integrity of the voting processes, including the accuracy of the vote tally process, as implemented by the Unity Voting System as currently used within the State of Ohio. Testing was performed at the State of Ohio Computing Center (SOCC) in Columbus, Ohio on equipment supplied by the State of Ohio.

The testing process included examination of the Unity Voting System's functionality related to defining an election, electronic and paper ballot configuration, installation of the election definition on the system's voting components, casting predetermined test ballots on the system's voting components, and collection, consolidation and reporting of the test ballots cast. Additionally, administrative and audit logging functionalities of the various system components were also examined.

Testing was conducted using the State Of Ohio's standard "Ohio Famous Names" (OFN) election definition. The OFN election definition was created using the Unity Election System's Election Data Manager (EDM) software application. The election definition was created in the SOCC by an ES&S associated representative during the course of training SysTest Labs and Ohio Secretary of State personnel in the configuration and usage of the Unity Voting System.

The OFN election definition was configured for voting in three precincts, one of which consisted of three splits. The election definition consisted of five individual ballot styles, and included five contested offices, one board election, one ballot issue question, and two School Board contests, each of which were limited to one sub-precinct of the split precinct.

The three precincts established in the SOCC for testing the Unity Voting System each consisted of two iVotronic DREs, one M100 precinct optical ballot scanner, and one AutoMARK ADA-compliant paper ballot marking device. Additionally, the test election definition was installed on a single M650 central office ballot optical scanner. The test environment was complemented by a single installation of the Unity Voting System's election management software on a machine common to all three of the configured precincts. The three test precincts' configurations were as dictated by staff of the Ohio Secretary Of State's office. While the three test precincts' configurations did not invalidate the test processes or results, they also did not accurately represent the way in which the Unity system is typically deployed in Ohio. The Unity system is typically deployed in Ohio as either iVotronic DREs, or M100 ballot optical scanners; precincts do not typically have both iVotronic DREs and M100 scanners. As a result of the configurations of the test precincts, the tests conducted were perhaps more comprehensive than they may have otherwise been.

Test cases included:

- Conducting an inventory of the provided Unity system components
- Physically setting up and configuring the Unity system components
- Observing the creation of the OFN election database
- Installing the OFN election definition on all of the voting hardware
- Printing and using Ballots On Demand ballot printing functionality
- Voting accuracy testing of all of the voting hardware
- Collecting and consolidating all of the cast ballots' votes
- Verifying entries to the Voter Verifiable Paper Audit Trail (VVPAT)
- Exercising administrative functionalities of the system components
- Capacity testing of the various Unity system media and memories
- Examining Audit Log entries made by the Unity software.

SysTest Labs also attempted to verify that the versions of the Unity Voting System applications provided for testing were the same as the official versions deployed in the State of Ohio. SysTest Labs generated SHA1 hash codes for the various Unity applications' installation packages for comparison to comparable hash codes derived for the State's official installation distribution. The State, however, was unable to provide an official installation distribution against which to compare SysTest's findings.

3.4.2.1 Test Case Results

SysTest Labs recorded an inventory of the ES&S Unity Voting System components provided by the State for testing. The components provided, both hardware and software, were in agreement with the versions documented as being in version 3.0.1.1 the Unity system.

The process of physically setting up and configuring the voting hardware was as described in the Unity system documentation. The M100 optical scanners were readily attached to the ballot boxes to which they secured. It was noted, however, that two of the three provided ballot boxes did not include write-in ballot diverters. The diverters are intended to segregate ballots containing write-in votes from those that do not include write-in votes. The diverters' absences will necessitate election workers having to search through the ballot boxes' contained ballots in the event of write-in votes having been cast.

The iVotronic DREs unfolded and stood up as also described in the system documentation. The iVotronic DREs are held upright by latches that are attached beneath the iVotronics' terminal screens. The latches that hold the screens up may not be strong enough to support an iVotronic. If an iVotronic screen in the upright position is pulled from the front it will collapse forward. Additionally, spring catches are built into the legs of the iVotronic stand to assist in holding its feet wide for support, but those catches are ineffective. The whole iVotronic apparatus, stand and machine, is top heavy, and there is a risk of one collapsing onto a poll worker or voter. Poll workers should be vigilant to ensure that no voter attempts to move, pull, or lean on an iVotronic during the voting process.

The Unity Voting System's election management software was successfully installed by following the instructions as presented by the ES&S associated training representative. The instructions as presented were compared to the installation documents and found to be in agreement. The Unity Voting System's election management applications are installable without problems by following the ES&S provided software installation documentation.

Installing the OFN election definition on the Unity system's voting components is as described in the system's documentation. There are, however, many potential risks that may be encountered by the typical user. The election definition is installed onto an iVotronic DRE by use of two media; a supervisor PEB, and a compact flash (CF) card. The contents for the PEB and CF are prepared through the use of Election Data Manager (EDM) and iVotronic Image Manager (iVIM), two applications within the Unity election management system. A third application in the Unity election management software, Hardware Programming Manager (HPM), is used to load the election definition into the PEB and CF. The iVotronic DRE is available in two screen sizes, 12 inches and 15 inches. The ballot images configured and generated within iVIM are not compatible with both screen sizes. iVIM allows ballot images for both screen sizes to be created within the same election, but only the last display's generated ballots are available to be copied to a PEB for transport to an iVotronic DRE. If ballot images for both screen sizes are both existent in an election within iVIM, then care will be needed to ensure that the correct screen size has been the last one generated for installation. This is a possible risk to the efficiency of configuring an election, not to the integrity of the voting process. Additionally, one should not attempt to display a ballot on an iVotronic DRE without first installing the CF card into the terminal. The CF card's contents include the images and text that comprise the visual aspect of the ballot display, and attempting to display the ballot without the CF card in place may result in crashing the firmware. If the firmware crashes and the iVotronic DRE then emits a continuous high-pitched tone; removing and reinstalling the battery will return the terminal to a normal state.

Installing the election definition on the M100 precinct ballot optical scanners was accomplished by following the instructions in the Unity system's documentation.

An election definition is installed on an M100 scanner by use of a PCMCIA flash card. The creation of the ballots' scan image was accomplished with ES&S Image Manager (ESSIM), an application within the Unity election management system. The ES&S associated training representative created the M100's ballot image within ESSIM during training conducted at the SOCC. An error not described in the system documentation was encountered when attempting to write the M100's ballot image to the PCMCIA flash card. The error was encountered in HPM and read: "Write error. Read-back failure." The encountered error was indicative of faulty PCMCIA flash cards. The cards were replaced by additional stock, and the election definition was then successfully loaded onto the M100 scanners.

The election definition was loaded onto the M650 central office optical scanner as described in the Unity system's documentation. An election definition is installed on an M650 scanner by use of a Zip disk. The ballot image used by the M650 is the same as that used by the M100. The Unity application, HPM, is also used to write the ballot image to the Zip disk for installation into the M650. An error was also encountered in HPM when attempting to load the ballot image onto the Zip disk for the M650. The error became manifest within HPM in the dialog used to specify the drive letter for the attached Zip drive to be used to write the Zip disk. The list of possible drive letters was populated with multiple, repeated and incorrect choices of drive letters. Exiting the HPM application, verifying that the Zip drive was properly connected to the Unity workstation, and then restarting HPM allowed error to be bypassed.

The election definition was also installed on three AutoMARK Voter Assist Terminals (VAT), which are ADA compliant paper ballot marking devices. An election definition is installed on an AutoMARK VAT by use of another CF card. The CF cards used in the iVotronic and in the AutoMARK VAT have different contents, are not interchangeable once written to. The OFN election definition was imported into the AutoMARK Information Management System (AIMS) software application, which is distributed as part of the Unity election management system, by following the instructions contained in the AIMS Election Officials Guide. The election definition was then written to the CF card, the process for which is also described in the AIMS Election Officials Guide.

The term "Ballots on Demand" (BOD) describes an optional function in ESSIM that allows paper ballots to be printed as needed during the course of an election. The ballots printed through ESSIM's BOD function must be readable by both of the M100 and M650 scanners, and also by the AutoMARK VAT. The BOD functionality of ESSIM was tested by printing 10 of each ballot style defined in the OFN election on the ES&S prescribed Okidata 9600 printer at the Franklin County Board of Elections warehouse.   One of each ballot style was then marked by hand, and another of each ballot style was marked using an AutoMARK VAT. All ten of the marked ballots that were printed through BOD were then processed through an M650 central scanner and the vote results were verified to be as expected. The ten marked ballots were then scanned on a single M100 precinct scanner for which an "Absentee" polling place had been added to the election definition, and to which all three defined precincts had been added. The results of processing the ten BOD ballots through the M100 scanner were also compared to the expected results and verified to be in agreement.

There were minor anomalies noted in the BOD software. In BOD mode within ESSIM, when adding Ballot Styles in the "Ballot On Demand Batch Ballots" dialog, after clicking the 'Add' button and displaying the "Ballot Quantity Selection" dialog, the 'Ballot' drop-down list would not stay displayed when first opened. It had to be opened a second time before it stayed open and allowed a selection to be made. And, on the same "Ballot On Demand Batch Ballots" dialog, the label at the bottom of the dialog read "5 Total Ballots for 5 Precincts", even though in the OFN election definition there were 5 ballots defined and added to the current batch for only 3 precincts.

A series of predetermined ballots was cast on all of the iVotronic DREs and M100 and M650 scanners to test the system's voting accuracy. Seventy-five predetermined ballots were cast on each of the six iVotronic DREs. Thirty-six predetermined paper ballots of each ballot style, 18 marked by hand and 18 marked by AutoMARK VATs, were each processed through both the M100 and M650 scanners ten times. A total of 450 ballots were cast on iVotronic DREs, and 3,600 paper ballots were scanned, 1,800 by each model of scanner. Results reports were produced by each piece of system hardware, the iVotronic DREs, the M100s, and the M650, and verified to be in agreement with the expected results.

3.4.2.2 Volume Testing

Accuracy is tested during qualification, but not when the capacity of the system is stretched to its limit.

A ballot was scanned through an M100 precinct ballot optical scanner 53,230 times. The vote counters on the M100 did not overflow. It is evident that the ballot counters allocated for use in the M100 are at least two bytes in size and therefore have a minimum capacity of 65,535.

It was determined that the maximum count of ballots that can be processed on an M650 central office scanner in a single precinct total is 65,535 ballots. This only confirms what ES&S says in their limitations document:

"No more than 65,535 votes can be tabulated for any candidate, over-vote or undervote in any precinct nor can the ballot count in a precinct exceed 65,535."

If a single precinct reaches that total no counts are incremented for any precinct included in the current election. When the 65,536th ballot is saved for a precinct, the M650 prints a message to its audit log that reads:

"Counters have reached their maximum. Counters restored to last Batch Save."

The same message is also displayed on the M650's display. At that point the M650's internal counters retain their last prior values as of the last prior successful save. There is a risk in that the message regarding the counters is not shown until the scanned ballots are saved, at which point it would not be known which ballot in the last processed batch was the first one not counted. The scanner keeps scanning with no warning until the scanned batch is saved to the internal hard drive by pressing the "Save" button. This issue can be mitigated by stopping saving results to a single zip disk prior to reaching the maximum count for any one precinct, then zeroing the internal counters, re-starting scanning, and saving the subsequent results to an additional zip disk for tallying by ERM.

The iVotronic DREs maintain vote data in three separate and redundant internal memories. ES&S would not provide information or support related to conducting volume testing of either the iVotronics' internal memories or the PEBs that are used for vote data transport.

3.4.2.3 Documentation

While counties' Boards of Elections staff may become skilled users of the Unity Voting System, the system's flexibility and complexity cannot be minimized. Understanding that training is provided by ES&S on their voting system, User Manuals/Guides and other documentation will be needed to conduct an election such as setting up the system at the Central Count and Poll locations, creating elections using the vendor's Election Data Manager (EDM), creating media for the various precinct hardware using Hardware Programming Manager (HPM), and consolidating votes for final tally using Data Acquisition Manager (DAM) and Election Reporting Manager (ERM). While testing at the State of Ohio Computing Center, SysTest Labs used the ES&S published system documentation as a reference in configuring and operating the Unity Voting System. It was found that the Unity system was complex and was not an intuitive system.

The physical setting up of the ES&S hardware is relatively simple. The iVotronic voting terminals' legs unfold into place in an easy to perform manner, but there are risks related to the strength of the supporting latches. The M100 precinct optical scanners attach easily to their supporting ballot boxes.

3.4.2.4 Unity Workstation Applications

The Unity Voting System's Unity workstation applications are used to create election definitions (Election Data Manager), create paper and DRE ballot images (ES&S Image Manager and iVotronic Image Manager), load election definitions onto portable media (Hardware Programming Manager), transfer results (Data Acquisition Manager), consolidate and report vote tallies (Election Reporting Manager), and view audit log information (Audit Manager).

3.4.2.5 Audit Manager

Audit Manager is used to configure and view audit log information related to election creation in Election Data Manager, and paper ballot configuration in ES&S Image Manager. Audit Manager contains a configurable option to disable, or turn off, audit logging functionality in those two Unity applications. When audit logging is disabled in Audit Manager it is not identified as such in either of the two applications. Audit logging must be enabled during the election creation and ballot configuration processes.

3.4.2.6 Election Data Concurrency

Concurrency problems across the Unity Election System's components can be caused by a failure to maintain all aspects of an election within the applicable Unity applications. Changes to the election definition in EDM require subsequent changes in the HPM and ERM applications, and also in the iVIM application if iVotronic DRE terminals will be used, and in the ESSIM application if paper ballots will be used. The order in which changes are made in the different applications is critical to maintaining the concurrency of the different system components. Failure to make required changes in the correct order after election definition modification may result in either or both of incorrect voter terminal and paper ballots, and might also result in incorrect results consolidation and reporting.

3.4.2.7 iVotronic Image Manager (iVIM)

If multiple ballot images have been defined in iVIM, and they are all generated so that all can be prepared for iVotronic, then the PEB that gets written to through the Hardware Programming Manager may not be compatible with a particular iVotronic as the PEB may contain ballot images of the wrong display size. While multiple ballot displays are allowable in iVIM as part of the same election, the user should be aware that only the most recently generated display image is written to the PEB. If the last generated display in iVIM is of the incorrect screen size for the iVotronic that the PEBs are being written for, invalid PEBs will not become known as invalid until loading the generated ballot images onto an iVotronic. This issue may become manifest in the case of a jurisdiction having both 12 and 15 inch iVotronics, and may also be an issue if an incorrect ballot image template size is selected in iVIM. Unity users must be careful to select the correct ballot image templates in iVIM, and iVotronics must be tested for being able to correctly display their installed ballot images prior to being placed in the field for voting.

3.4.2.8 Data Acquisition Manager (DAM)

Data Acquisition Manager (DAM) is not used in Ohio for modem communications, but one county does use it to read vote results from PEBs and onto the Unity workstation, instead of using Election Reporting Manager to read the PEBs. Our test of voting accuracy and reporting included reading one of our three precinct's votes by use of DAM. There were no issues noted in reading the PEB by use of DAM.

3.4.2.9 Ballots on Demand (BOD)

The tested version of ES&S Image Manager, which was supplied by ES&S and should have been identical to the official Ohio version, did not have Ballots On Demand enabled. ES&S provided an alternate copy of file [redacted]' that when dropped into folder C:\[redacted], replacing an existing version of the file, did allow ESSIM to come up in BOD mode. Therefore, the installation of Unity 3.0.1.1 that ES&S provided for testing was not identical to the Ohio approved version.

In BOD mode for ES&S Image Manager, when displaying the "Ballot On Demand Batch Ballots" dialog, the label at the bottom of the dialog read "5 Total Ballots for 5 Precincts", even though for the test election there were 5 ballots defined and added to the current batch for only 3 precincts.

The BOD functionality of ES&S Image Manager was tested by printing 10 of each ballot style defined in the Ohio Famous Names election on the ES&S prescribed Okidata 9600 printer at the Franklin County Board of Elections warehouse. One of each ballot style was then marked by hand, and another of each ballot style was marked using an AutoMARK Voter Assist Terminal. All ten of the marked ballots that were printed through BOD were then processed through an M650 central scanner and a M100 precinct scanner, and the vote results were verified to be as expected.

3.4.2.10 Hardware Programming Manager (HPM)

An error not described in the system documentation was encountered when attempting to write the M100's ballot image to the PCMCIA flash card using HPM. The error was encountered in HPM and read: "Write error. Read-back failure." The encountered error was indicative of faulty PCMCIA flash cards. The cards were replaced by additional stock, and the election definition was then successfully loaded onto the M100 scanners.

A programming error was also encountered in HPM when attempting to load the ballot image onto a Zip disk for the M650 central scanner. The error became manifest within HPM in the dialog used to specify the drive letter for the attached Zip drive to be used to write the Zip disk. The list of possible drive letters was populated with multiple, repeated and incorrect choices of drive letters. Exiting the HPM application, verifying that the Zip drive was properly connected to the Unity workstation, and then restarting HPM allowed error to be bypassed.

3.4.2.11 Election Reporting Manager (ERM)

ERM allows importing M650 results zip disks multiple times; it doesn't write anything to the disks or have any other controls to prevent the reading into ERM of the same results zip disks multiple times. Mitigation has to be a procedural issue in the central count office that describes controls to preclude importing from the same zip disk multiple times.

As described in the "Limitations of the Unity 3.0.1.1 System" document as provided by ES&S, ERM cannot display vote totals on a precinct detail report in excess of 99,999 from any one tabulation source in a precinct. If exactly 100,000 votes are reported from any one tabulation source for a precinct then 0 (zero) will be displayed in the precinct detail reports instead of the correct value. If a vote total in excess of 100,000 is reported from any one tabulation source for a precinct then only the amount in excess of 100,000 will be displayed in the precinct detail reports. This restriction applies only to the reported vote totals from individual tabulation sources as those fields are documented in Appendix B of the "Election Reporting Manager User's Guide" as "5 Position Numeric" fields. The reported "Total Votes" sum from all tabulation sources, documented in

Appendix B as "7 Position Numeric," is capable of displaying in excess of 100,000 votes. Mitigation of this issue on the precinct detail reports may require advance planning in creating precinct detail reporting groups within the Unity applications.

3.4.2.12 Administrative User Names and Passwords

The Unity applications generally have the same default administrative User Name and Password combinations, "[redacted]"/"[redacted]" or "[redacted]"/"[redacted]". County Boards of Elections generally do not change the default combinations. Security risks should dictate that those default combinations should be replaced and disabled.

3.4.2.13 AutoMARK Voter Assist Terminal (VAT)

The AutoMARK VAT is an ADA-compliant ballot marking and reading device not manufactured by ES&S, but made compatible with ES&S Unity Voting System election definitions.

3.4.2.13.1 Erratic Scrolling

The VAT's display scrolling of a zoomed ballot became erratic after the brail caption buttons was used. The display sometimes scrolled by whole race boxes, and at times made it impossible to completely see the contents of a race's display box. The race's title may have been seen, but the selected candidate might not have been displayable through scrolling. This problem was only noted after using the brail captioned physical buttons on the face of the machine. Ejecting and re-inserting the ballot corrected the display problem. When the brail buttons were not used, and only the on-screen navigation bars were used, the display scrolled correctly allowing the entire ballot to be displayed.

3.4.2.13.2 Undocumented Error

During ballot marking on an AutoMARK model A100-00 an error message was displayed that read:

"Alert! A problem has occurred. Please notify an election official.
There was an error while printing."

The specific error text could not be found in the AutoMARK documentation. The instructions from page 29 of the "AutoMark Poll Workers Guide VAT 1.1.pdf" for the "general error" were followed. The instructions described turning the marking machine off, and then turning it back on. The machine restarted normally and ejected the unmarked ballot that had been placed into it prior to the error occurrence.

3.4.2.13.3 Ballot Recognition

While the AutoMARK VAT correctly recognized and rejected ballots from the wrong precinct, a precinct not on its compact flash card, the AutoMARK did not always recognize an inserted ballot that was from the correct precinct. Ballots from the correct precinct were recognized as such and accepted on the second or third ballot insertions.

3.4.2.13.4 Write-In Keyboard Character Sets

The keyboard screens displayed to enter write-in votes on the AutoMARK have different character sets than the equivalent screens on the iVotronic DRE. The iVotronic DRE's write-in keyboard display includes period (.) and comma (,) characters, and the AutoMARK’s display omits those two characters. The difference in the available character sets may result in vote consolidation errors.

3.4.2.14 iVotronic DRE

The iVotronic is the Unity Voting System’s DRE device. The iVotronic comes in multiple physical configurations including 12 and 15-inch models, and ADA and non-ADA compliant models.

3.4.2.14.1 Physical Set-Up

The iVotronic DREs unfolded and stood up as described in the system documentation. The iVotronic DREs are held upright by latches that are attached beneath the iVotronics’ terminal screens. The latches that hold the screens up may not be strong enough to support an iVotronic. If an iVotronic screen in the upright position is pulled from the front it will collapse forward. Additionally, spring catches are built into the legs of the iVotronic stand to assist in holding its feet wide for support, but those catches are ineffective. The whole iVotronic apparatus, stand and machine, is top heavy, and there is a risk of one collapsing onto a poll worker or voter. Poll workers should be vigilant to ensure that no voter attempts to move, pull, or lean on an iVotronic during the voting process.

There is a power strip inside the iVotronic stand that must be connected to and switched into the 'On' position before the iVotronic screen is placed and locked into position or the RTAL will not work, even though the iVotronic will itself operate on battery power. If the power strip in not switched on the error may be manifest by a message displayed on the iVotronic describing the lack of its RTAL printer.

3.4.2.14.2 Real Time Audit Log (RTAL) printer

The printer connector to the iVotronic does not screw into place and may be easily removed by any voter and left in a position that its removal may not be obvious. In that event the iVotronic will not accept additional votes, and will display a message identifying its RTAL printer not being connected as the problem. In that event the solution is to properly reattach the RTAL printer connector.

There is a physical risk that during a routine change of printers between the RTAL and the Seiko report printer that somebody will bend a pin on a serial connector. The mitigation is, as usual in such circumstances, be very careful in making the connections, and have replacement serial cables accessible.

3.4.2.14.3 Administrative Passwords

iVotronic passwords for the different administrative menus and functions are the same across the election as documented in the file "Unity Default Passwords - FYIMSC0015.pdf", which was provided on the 3.0.1.1 installation disc, although the iVotronic passwords are editable for the election within Election Data Manager. The iVotronics that were provided for testing still all had the default passwords as valid. Election officials should change the passwords occasionally for security reasons.

3.4.2.14.4 Undocumented Logic and Accuracy Test Option

The "iVotronic Operator's Manual 9.1.pdf" that was supplied from ES&S does not describe an option in the "Automated Vote Selected Ballot Test" Logic and Accuracy test. The manual reads: "The largest number that can be requested is 12,999", but when accessed on the iVotronic there was an option to "Fill Memory" that is not described in the manual.

3.4.2.14.5 Report Printing

The iVotronic does not detect when its report printer goes off-line, is disconnected, or turned off during report printing. The user must be aware of what's being printed and what the printed report's expected contents should be, and be cognizant of the printer's status to assure that reports are printed in their entireties. If a report fails to print in its entirety then the user should be ready to re-print the report.

3.4.2.14.6 Display Issues on the 12-Inch iVotronic

During the course of conducting tests at the SOCC, a report from one of Ohio’s counties indicated that an error was encountered in the field when attempting to load ballot images for a split precinct onto a 12-inch iVotronic DRE. This claim was investigated in the SOCC by loading the Ohio Famous Names election definition’s split precinct’s ballot images onto a 12-inch iVotronic DRE. There was no evidence of any problem being encountered in doing so. It is suspected that possibly the problematic iVotronic ballot images in the field were created to be of the wrong size, as described above, in iVIM.

On the 12-inch iVotronic DRE, on the Write In screen, the instructions to the voter are not entirely visible. The first two lines of the instructions overlap, and the text entry box completely obscures the last line of the instructions, only the tops of the characters of which are barely visible at the top of the text entry box overlay. The last line of the instructions to the voter read: "Please Accept or

Cancel when you are done." The instructions are fully visible on the 15-inch iVotronic DRE.

3.4.2.15 M650 Central Ballot Optical Scanner

3.4.2.15.1 Ballot Processing

The M650 scanner does not mark ballots to identify them as counted. Scanner operators must be extremely careful in following procedures written to prevent duplicate scanning of ballots. Ballots should be processed in batches in their entireties, and batches of scanned ballots must be physically segregated away from un-scanned batches to prevent confusion as to ballots' scanned statuses.

3.4.2.15.2 Ballot Data Saving

The M650 requires a manually executed save procedure to write scanned vote data to its internal hard drive. If power is lost during the scanning process then it becomes necessary to re-scan any ballots processed since the last prior save. It is critical that batches be processed in their entireties, with very methodical saves performed, or there is a real danger of duplicate scanning of ballots, or of omitting some ballots from the scan process entirely.

3.4.2.15.3 Ballot Oval Orientation

The M650 is constructed to read only left ovals or right ovals. The model provided for testing was constructed to read left ovals. ESSIM allows the user to specify right or left sided ovals in the ballot definition. There is a risk that ballots with ovals on the wrong side could be printed and therefore be unreadable by an M650. It would be a user error, but there is a risk. The mitigation is to be very careful using ESSIM, and to not specify ballot ovals on the incorrect side for the configuration of the M650 to be used.

3.4.2.15.4 Zip Disk Capacity

The M650 had a completely full zip disk inserted into it. When it was attempted to store vote information to it, the M650 displayed the following: "Error: Could not Run Copy Command!", and also printed to its audit log printer: "System Could not Run cp (copy)." The displayed error message is as documented on page 58 of the M650 Operator's Manual. .

3.4.2.16 M100 Precinct Ballot Optical Scanner

3.4.2.16.1 Ballot Auto-read Option

To determine the number of bytes used to store vote counts on the M100's PCMCIA flash card, and therefore the maximum vote total allowed for any single ballot position, the M100's Ballot Auto-read Option was used. The results reports showed that the results for the single ballot issue question were being mis-reported for the incorrect response. The ballot scanned repeatedly had "No" marked for the issue question, but the results showed every vote on that item as "Yes." The ballot images for the election's five ballot styles were examined in

ES&S Image Manager (ESSIM) and showed that the ballot positions for "Yes" and "No" were identical on all five ballot styles. The ballot issue question was not configured to rotate, so the election definition for that particular item was correct as written to the flash card for installation into the M100. It is not known if the Auto-read Option executes a different logical path within the M100's firmware than is executed during the course of normal voting. This is an item that may be referred to the manufacturer.

3.4.2.16.2 Report Printing

The manual "ES&S Model 100 Precinct Ballot Counter Operator's Manual" describes on page 45 that when the printer is out of paper:

"Note: A "time out waiting for paper" message may appear due to the internal printer being out of paper."

But, that message was only observed when the printer was out of paper when a report was requested. There was no out of paper warning or message when the paper ran out during the printing of a report. When the paper ran out during the printing of a report the printer continues printing to nothing; the print output is lost. The mitigation is two-fold; make sure that there is adequate paper in the M100 before running reports, and reprint any reports that may be truncated for having run out of paper.

3.4.2.16.3 PCMCIA Card Security

The M100's allocated ballot counter storage locations on the PCMCIA cards were located by using the PC Card Manager application to export the card's contents to files after scanning varying numbers of ballots, and comparing the captured data exports using UltraEdit-32, a product of IDM Computer Solutions, Inc. The PCMCIA card's ballot counters' values were edited, also using UltraEdit-32, and the PCMCIA card re-inserted into the M100 scanner. The M100 scanner's logic included a circular redundancy check (CRC), a mathematically derived verification of the card's contents, resulting in the M100's recognition that the card had been altered. The M100 would then not allow opening polls, or voting.

3.4.2.16.4 PCMCIA Card Capacity

It was determined that the M100 does not use additional memory on the PCMCIA memory card to record ballots scanned. The card's capacity beyond the election definition is used to write audit log entries.

3.4.2.16.5 Unreadable Marks

M100 did not scan incomplete marks reliably or consistently. Sometimes it recognized incomplete marks as votes, and sometimes it responded with messages describing "unreadable marks" when the ovals were marked with simple lines, or other incomplete marks, drawn in the ballot ovals, and sometimes described them as undervotes, when the same ballot was scanned. It is possible that clearly indicated votes may not be recognized by the scanner, and if the election is not configured to warn of undervotes, those votes will be lost. It's also possible that overvotes may not be recognized as such and warned about if made with marks that the scanner does not recognize. The condition of unreadable marks may be mitigated through multiple precautions. It is important that the "Model 100 Scanner Options" in the Hardware Programming Manager application be set to reject "Unreadable Marks", as described on page 26 of the "HPM 5.2 User Guide", in order for the M100 to provide voters warnings in the event of unreadable marks. Additionally, as described in the "ES&S Model 100 Precinct Ballot Counter Operator's Manual", darken unreadable marks on the ballot when they are reported as such. It is important that voters be educated about how to properly fill in ballot ovals. It is also important that the M100 scanners be properly maintained, including blowing debris from the paper ballot scanning path and read heads by using canned pressurized air as described on page 43 of the Operator's Manual.

3.4.2.16.6 Write-In Ballot Diverters

Of the three metal ballot boxes received for testing, only one had a write-in ballot diverter. Without the write-in ballot diverter, finding and tallying write-ins could be a difficult task. Additionally, it was observed that a ballot slid under the diverter in the one ballot box that was so equipped.

3.4.2.17 Preliminary Mitigation Tactics

1. Documentation must be available and updated
2. Vendor support must be bought by the counties
3. All peripherals must be bought from the vendor

3.4.2.18 Conclusions

The Unity Voting System, as deployed within the State of Ohio, is fully capable of being used to accurately assess and tally the public's vote in a major election. The Unity Voting System, however, is not a fully integrated system. The election definition, ballot creation, results consolidation and reporting processes are not highly integrated functionally with the Unity Voting Systems suite of software applications. The Unity Voting System's election management software may be best described as a collection of applications that operate on related data. The Unity applications do not have a single user interface, nor are the various applications' user interfaces uniform, and changes made to an election definition are not propagated through the various applications' data without additional user intervention. In a full and complete deployment, the Unity election system employs four different types of electronic media containing five different sets of data content to transfer election information to its various voting components. The five sets of data content required to keep the Unity system's voting components concurrent for an election are maintained by use of five separate software applications, Election Data Manager (EDM), iVotronic Image Manager (iVIM), ES&S Ballot Image Manager (ESSIM), Hardware Programming Manager (HPM), and AutoMARK Information Management System (AIMS). Additionally, for results to be correctly collected and reported a sixth applications, Election Reporting Manager's (ERM), related data needs to be separately maintained as an election definition is modified. Data concurrency problems between the Unity Voting System's components can be caused by a failure to maintain all aspects of an election within the applicable Unity applications. Changes to the election definition in EDM require subsequent data maintenance in the HPM and ERM applications, and also in the iVIM application if iVotronic DRE voting terminals will be used, and in the ESSIM application if paper ballots will be used. The order in which data maintenance is performed in the different applications is critical to maintaining the concurrency of the different system components. Failure to perform required data maintenance in the correct order after election definition modification in EDM may result in either or both of incorrect voter terminal and paper ballots, and may also result in incorrect voting results consolidation and reporting.

Paper ballot processing in the Unity Voting System must be carefully controlled. Paper ballots do not have encoded identification to prevent ballots from being processed multiple times, or to allow for automated detection of missing ballots.

Ballots scanned through a M100 precinct scanner are deposited directly into a locked ballot box, and the accumulated vote totals are stored in non-volatile memory on the inserted PCMCIA flash card.

Ballots processed through a M650 central office scanner are not deposited directly into a secure ballot box. It is very important that procedures be in place to describe the handling of ballots processed through a M650. Votes processed by a M650 are not stored in non-volatile memory within the machine until the user performs a manual data save operation. If a M650 scanner suffers a power failure during the scanning process, then all ballots scanned subsequent to the last manual data save operation must be reprocessed. If such ballots are not reprocessed then those votes will not be counted. It is very important each time a manual data save operation is performed that the just processed ballots be moved to a secure location physically segregated from the unprocessed ballots. Ballots should be aggregated into batches, and batches should be processed in their entireties to prevent confusion as to what has and hasn't been processed.

It is equally important that procedures describe the handling and importing of vote results from M100 and M650 scanner media into the Election Reporting Manager application. There are no safeguards inherent in the system to prevent a user from importing vote results from the same memory device multiple times. System operators should store processed memory devices in a secure location physically segregated from unprocessed media devices immediately after processing them.

Table 18 ES&S Performance Test Risk Assessment Table of Results

ID	Probability of Occurrence	System Impact Level	Risk Assessment	Risk	Mitigating Factors
PERF-ESS-1	C	2	**YELLOW**	IVotronic physical stability is fragile. After many	Counties should include a full inspection of each

ID	Probability of Occurrence	System Impact Level	Risk Assessment	Risk	Mitigating Factors
				election cycles the stability of the iVotronic Unit is compromised due to worn parts which make the unit susceptible to tipping over and damaging itself. Could result in polling place not having enough DREs for voters.	iVotronic unit as part of their Pre-Election process.
PERF-ESS-2	D	2	**YELLOW**	RTAL power supply is concealed in the iVotronic unit which is not apparent to pollworkers. RTAL not being connected to power supply could lead to pollworkers believing a defective unit was delivered and not be used in election.	Pollworkers should include a full inspection of each iVotronic unit as part of their Pre-Election process.
PERF-ESS-3	D	2	**YELLOW**	Unity does not mandate that passwords need to be changed. Default passwords (to access voting equipment during election) are set within Unity. This could result in unauthorized personnel to change settings on Voting equipment	State must mandate that all passwords need to be changed and only revealed to necessary personnel.
PERF-ESS-4	D	2	**YELLOW**	Changing the printers on the iVotronic may result in a bent pin	Training must be updated to emphasize the danger and possibility of this occurrence.
PERF-ESS-5	C	3	**YELLOW**	iVotronic reports are lost if the report printer is disconnected	Be prepared to re-print reports if needed
PERF-ESS-6	B	3	**YELLOW**	Write-in instructions are not fully displayed on the 12" iVotronic. This could lead to write-in not entered and voter discontent.	Supplemental instructions should be provided at the polling location.
PERF-ESS-7	C	3	**YELLOW**	Some M100 ballot boxes lacked a diverter, this could result in delay tallying the write-ins.	Counties should include a full inspection of each M100 as part of their Pre-Election process.
PERF-ESS-8	C	3	**YELLOW**	M100 does not scan incomplete marks consistently.	Post instructions at all polling sites for voters to completely darken intended ballot ovals as per documentation
PERF-ESS-9	A	1	**RED**	Paper ballots can be scanned more than once. M100 and	Process batches in their entirety, and have

ID	Probability of Occurrence	System Impact Level	Risk Assessment	Risk	Mitigating Factors
			🟥	M650 scanners do not mark ballots as processed. A person with malicious intent can skew the election results.	handling procedures in place such as a D and an R present.
PERF-ESS-10	C	3	**YELLOW**	M100 does not detect when printer paper runs out during printing. Could result in a delay of the election process.	Training should be updated to note this. And to verify there is adequate paper
PERF-ESS-11	A	2	**RED**	M650 requires a manual save procedure to save scanned ballots information from the internal RAM. A power failure will result in RAM memory being lost i.e. the scanned ballots. Ballots will have to be res-scanned.	Process batches in their entireties; establish a policy to save data regularly and often.
PERF-ESS-12	D	2	**YELLOW**	M650 only reads ovals in either the right or left columns. This could result in ballots not being read correctly	Verify counties will create ballots with the correct template in ESSIM
PERF-ESS-13	C	3	**YELLOW**	AutoMARK does not always recognize the inserted ballot. User needs to Eject and re-insert ballot. This will cause voter discontent, confusion, and loss of confidence.	Supplemental Instructions should be provided at polling location. Pollworker education is essential.
PERF-ESS-14	C	3	**YELLOW**	iVotronic and AutoMARK do not have identical character sets in their write-in keyboard displays. This will delay reporting results.	Review and reconcile write-in votes
PERF-ESS-15	C	3	**YELLOW**	AutoMARK's display scrolling becomes erratic will cause voter discontent, confusion, and loss of confidence.	Supplemental Instructions should be provided at polling location. Pollworker education is essential
PERF-ESS-16	E	2	**GREEN**	HPM displayed a 'read back error' when writing M100 PCMCIA cards.	Use a different PCMCIA card. Cards sent by the BOE had been damaged; appeared slightly dented. Cards need to be examined and tested before all elections.
PERF-ESS-17	E	2	**GREEN**	In the event a voter should press the two outer buttons on the M100 while entering	Vendor software/firmware fixes to disable the buttons

ID	Probability of Occurrence	System Impact Level	Risk Assessment	Risk	Mitigating Factors
			🟩	their ballot – very unlikely scenario due to the covered paper guide – the poll will close.	during voting. Pollworker training issue/alert

3.4.3 Hart InterCivic

The SysTest Labs' risk assessment team executed a voting system specific test plan to assess the usability and accuracy of the Ballot Origination, Tally, Rally & Servo system as deployed within the State of Ohio. Tests of the devices used to record ballots cast including eSlate direct record electronic (DRE) voting terminals and the eScan precinct ballot optical scanners were included in the executed test plan.

The Ballot Origination, Tally, Rally & Servo System is not as feature rich a voting solution as ES&S or Premier and as such, does not the flexibility in election definition and ballot design capabilities. In turn, this makes the Hart system are far less complex solution with fewer potentials for risks.

The objective of SysTest's assessment was to identify potential risks to the integrity of the voting processes, including the accuracy of the vote tally process, as implemented by the Ballot Origination, Tally, Rally & Servo System as currently used within the State of Ohio. Testing was performed at the State of Ohio Computing Center (SOCC) in Columbus, Ohio on equipment supplied by the State of Ohio.

The testing process included examination of the Ballot Origination, Tally, Rally & Servo System's functionality related to defining an election, electronic and paper ballot configuration, installation of the election definition on the system's voting components, casting predetermined test ballots on the system's voting components, and collection, consolidation and reporting of the test ballots cast. Additionally, administrative and audit logging functionalities of the various system components were also examined.

Test cases included:

- Conducting an inventory of the provided Ballot Origination, Tally, Rally & Servo system components
- Physically setting up and configuring the Ballot Origination, Tally, Rally & Servo system components
- Creation of the election definition database
- Installing the election definition on all of the voting hardware
- Voting accuracy testing of all of the voting hardware
- Collecting and consolidating all of the cast ballots' votes
- Verifying entries to the Voter Verifiable Paper Audit Trail (VVPAT)
- Exercising administrative functionalities of the system components

- Capacity testing of the various Ballot Origination, Tally, Rally & Servo system media and memories
- Examining Audit Log entries made by the Ballot Origination, Tally, Rally & Servo software.

SysTest Labs also attempted to verify that the versions of the Ballot Origination, Tally, Rally & Servo System applications provided for testing were the same as the official versions deployed in the State of Ohio. SysTest Labs examined the directory tree structures and file sizes of the software loaded on the servers and compared these to expected results. The State, however, was unable to provide an official installation distribution against which to compare SysTest's findings.

3.4.3.1 BOSS Functionality

BOSS is the Election Management System created by HART.

3.4.3.1.1 Translation of Text and Audio Files

The process to create audio translation from text files requires user to leave the Hart proprietary system and create folders and move files on Windows platform. This could result in overwritten files, misplaced files, or confusion if the user is working on multiple elections. It would be beneficial if process would be automated with unique and proper naming conventions for files.

3.4.3.1.2 Polling Place ID

BOSS auto generate the polling place ID within the system. It does not allow the user to roll back the polling place ID or make changes to the polling place ID. Although this is an internal function of the BOSS program, it can confuse the counties who track precincts by precinct number and may wish to correlate with the generated number sequence.

3.4.3.1.3 BOSS Ballot Text Word Wrap

Even though paper ballots are printed correctly, BOSS generates and prints ballots for review on the screen but the text does not word wrap correctly. This makes it difficult for the end user to proof the ballot for errors. This could result in lost time in preparing for the election.

3.4.3.2 Tally Database Versioning

Tally is the Hart Voting System tabulation software. Tally uses databases whose versions differ from the Tally application version number. The database opens within Tally as version 4.1.1 and once tabulated, they display version 4.7.3. Both Differ from Tally's version of 4.3.10. The variation in versioning could cause an administrator to believe incorrect version is installed on server. Hart InterCivic states the version number serves as a tool for internal engineering version control.

3.4.3.3 Sip-n-Puff

The eSlate Sip-n-puff unit is cumbersome and difficult for the poll worker to attach and detach.

3.4.3.4 PCMCIA Cards

A PCMCIA Card reader is supplied to download an election to an MBB. The user can easily insert the card in backwards. In which case pliers are required to remove PCMCIA card. This could cause PCMCIA card to be damaged.

3.4.3.5 Audit Log

The Audit Log did not record when the JBC unit was powered down. It does record when unit was powered up. This could hamper any inquiries if a re-creation of election-day events.

Table 19 Hart InterCivic Performance Test Risk Assessment Table of Results

ID	Probability of Occurrence	System Impact Level	Risk Assessment	Risk	Mitigating Factors
PERF-HRT-1	**D**	**3**	**Green**	Process to create audio translation from text files requires user to leave the Hart proprietary system and create folders and move files on Windows platform. Could result in previously created files to be overwritten if the user is working on multiple elections.	Automate the process to avoid user errors or provide improved standardized process.
PERF-HRT-2	**D**	**3**	**Green**	Polling place id in BOSS system auto numbering and does not allow user to roll back Precinct ID make changes on same ID. Could confuse counties tracking system for Precinct IDs	Allow flexibility or do not rely on BOSS assigned Polling place ID for tracking
PERF-HRT-3	**C**	**4**	**Green**	The print preview for the paper ballot displays the text not wrapping. However, prints perfectly fine. Could result in lost time in preparing the election	Supplemental documentation and/or training need to be provided to the person creating the election.
PERF-HRT-4	**C**	**3**	**Yellow**	One JBC cannot be used for Early Voting and Election Day processing. This will force small community to purchase 2	Do not allow Early Voting in precincts with 1 JBC.

ID	Probability of Occurrence	System Impact Level	Risk Assessment	Risk	Mitigating Factors
			🟨	JBC units.	
PERF-HRT-5	**D**	**3**	**Green**	Buttons on the front panel of the eScan Scanner are not labeled. This could confuse poll worker.	Supplemental documentation and/or training need to be provided.
PERF-HRT-6	**D**	**4**	**Green**	The TALLY v 4.3 uses internal databases with varying version numbers i.e. 4.1.1 and 4.7.3. This could lead the user to believe incorrect versions are installed. (versions are for HART purposes only)	Supplemental documentation and/or training need to be provided.
PERF-HRT-7	**C**	**4**	**Green**	The eSlate Sip-n-puff unit is cumbersome and difficult for the poll worker to attach and detach.	Require a pre-attached unit is delivered to polling location.
PERF-HRT-8	**D**	**4**	**Green**	Needed to use pliers to remove PCMCIA card that was accidentally backwards. This could cause PCMCIA card to be damaged.	Supplemental documentation and/or training need to be provided.
PERF-HRT-9	**A**	**4**	**Yellow**	JBC did not record the time unit was powered down in the audit log. Unit did record the time it is powered up. Therefore will not be able to determine how long the JBC was powered down. This could hamper any inquiries if a re-creation of election day events needs to be created.	Require constant monitoring of JBC units.

4. Suggestions for Improvement

In addition to the mitigation strategies outlined for each risk in Table 12 througfh Table 19, SysTest Labs offers the following suggestions for improvement for the critical risks identified in this study.

The Audit Log did not record when the JBC unit was powered down. It does record when unit was powered up. This could hamper any inquiries if a re-creation of election-day events.

Table 19 Election Operations and Internal Controls

The operational vulnerabilities identified by the Election Operations and Internal Controls team can be addressed and mitigated by the following suggestions. These suggestions are general in nature and more detailed countermeasures and mitigation strategies will be offered directly to the Secretary of State so as to not compromise existing security within counties.

1. A physical security assessment of each BOE facility should be conducted by a Physical Security and Crime Prevention Specialist from a local law enforcement agency. Suggestions, upgrades, security systems resulting from the assessment should be implemented.
2. An outline and standards for local procedures covering all election operations should be developed at the state level. Standards should also address inclusion of standardized, efficient and effective workflows for each voting technology and/or voting system. Counties should be required to develop resulting written procedures which should be reviewed and approved by peers and/or the Secretary of State. Periodic audits should be conducted to ensure counties comply with the procedures and that the procedures are updated to reflect changes.
3. Statutes, regulations and directives should be formally reviewed and revised with an emphasis on bringing them in line with current technologies and their new constraints and timelines. Specific area to examine include: timelines for inclusion of candidates, offices, measures and local options on the ballot; chain of custody and security of certified software and firmware changes, patches and upgrades; absentee ballot processing timelines and disqualifying criteria; and canvassing procedures and timelines.
4. Testing processes and protocols (e.g., Logic & Accuracy Testing) for each class of voting technology should be developed at the state level and monitored and enforced. A provision for external review of testing by the state or formal internal certification of the tests by the Board members should be part of the protocol.
5. Standardized job descriptions, merit based hiring/firing practices, minimum qualifications and on-going professional training should be developed at a state level and implemented at the local level. Such reforms can be made without sacrificing the partisan structure of the appointed local boards.

4.1 Configuration Management

1. Clear communication with the BOE personnel to ensure that they understand that using something other than specified materials may result in significant failures during an election.
2. Develop a centralized source for dissemination of information (L&A procedures, hardware/software compatibility information and user documentation).
3. Provide a means for creating and maintaining a centralized database of the field inventory by county containing manufacturer, model, serial number and revision level information of certified systems. The database would be readily accessible by county BOE personnel for verifying the revision levels of their equipment.

4.2 Performance Testing

4.2.1 Premier

SysTest Labs recommends that Premier provide a fix to the AccuVote TSx system that would preclude it from purging required files when the limit of the PCMCIA Card memory is reached. A workaround for this risk, until a code fixed can be implemented, is for Premier to determine what the fixed number of allowable votes per minimum PCMCIA Card memory allocation is and to provide this number to each County using the AccuVote TSx system. The County would then be able to ascertain if the number of voters and maximum number of potential votes would exceed to allowable limit for their PCMCIA Cards.

4.2.2 ES&S

Programmatic mechanisms should be developed and implemented in the unity Software that ensure that audit logging is always turned on by default during the election creation and editing process and operation. A workaround for this risk is to enforce policies for ensuring that the Audit Logging capability has not been disabled during election creation and editing process and operation.

4.2.3 Hart Intercivic

SysTest Labs believes that because the Audit Log does not record when the JBC unit is powered down; solely when it is powered up – that problems will occur recreating Election Day events. Hart Intercivic should address this as a software deficiency and a fix should be made available.

5. Summary

The SysTest Labs Ohio Voting Systems Risk Assessment for the EVEREST Project identifies and discusses the security, operational, management and regulatory risks to Hardware, Firmware, and Software Configuration Management; Election Operations and Internal Control; and, Performance and Usability identified during the assessment. These risks are specific to voting system, though not to any class of voting technology or county. Mitigation of these risks is not to be found in the voting technology certified by the state. Mitigation of these risks will largely be found in changes in poll worker education, management practices, organizational structures, workflows, budgetary appropriations, election official processes, legislation and directives at both the state and county level. The exceptions to the process driven solutions will require vendor activity. These are:

1. A mechanism to confirm the SHA-1 Hash codes in the BOE servers and polling place devices are compliant with the State of Ohio certified versions.
2. ES&S must change their software to not allow audit logs to be disabled.
3. Premier will need to make software fixes to the TSx so that once the device reaches capacity it disables its functionality. At present, it rolls back and deletes the vote’s folder.
4. It was noted that passwords were not being changed from the EMS system default. This allows all members of a BOE staff to have administrator privileges.
5. Extraneous software must be removed from the EMS servers. Commercial servers are packaged with software packages such as Microsoft Office and Internet Explorer. Such extraneous software can not reside on the same server used to process elections. Upon receipt of the server all software not directly related to the functionality of the EMS software must be removed. An image of the EMS software should be produced by the vendor, verified by the Secretary of State’s office, and installed on the county servers in accordance with the system in use.

Issues 2, 3 and 4 have process workarounds that maybe observed as a stop gap measure:

For Issue 2 - the disabling of the ES&S audit log; a checklist must be followed before and after every election to assure that the audit log is not disabled. Best Practice is to never disable the log – not for training or any other reason. It is realized that the logging activity slows the performance; still, this log has been turned off, in at least one county, and not restarted for the next election.

Regarding Issue 3 – Premier must make a software adjustment to the TSx due to the vote’s folder being deleted at capacity. A documented procedure to disable the device at 6000 amount of votes must be communicated and followed. This is a low number to assure the complicity of the ballot does not become an issue.

Issue 4 – A process must be put in place to force passwords to be identified with a user. The Best Practice is to change passwords before and after every election. To accomplish this process a checklist may be employed.

6. Terms and Abbreviations

These terms and abbreviations will be used throughout this document:

Table 20 - Matrix of Terms & Abbreviations

Abbreviation	Description
EAC	Election Assistance Commission
ITA	Independent Test Authority
NASED	National Association of State Election Directors
SOCC	State of Ohio Computer Center
SOS	Secretary of State
VSS	Voting System Standards
VVSG	Voluntary Voting System Guidelines
VSTL	Voting System Test Lab
Binary	Executable file, a "binary" file, containing machine code that is loaded into a memory device for the computer to execute.
BOM	Bill O Materials (BOM) are usually hierarchical in nature with the top level representing the sub-assembly or end-item. For example the end-item BOM for a Personal computer would list the computer, its major sub-assemblies (board, chassis, modem, keyboard, display, etc.).
CF	Compact Flash (CF) was originally developed as a type of medium used in portable electronic devices. For storage, Compact Flash typically uses flash memory in a standardized enclosure.
COTS	Commercially available Off The Shelf equipment (e.g., personal computers, printers).
Firmware	Firmware has evolved to mean the programmable content of a hardware device, which can consist of machine language instructions for a processor or configuration settings for a fixed-function device, gate array or programmable logic device. A common feature of firmware is that it can be updated post-manufacturing, either electronically, or by replacing a storage medium such as a socketed memory chip.
Hardware	Hardware is a general term that refers to the physical artifacts of a technology. It may also mean the physical components of a computer system, in the form of computer hardware.
PROM	An EEPROM (also called an E^{2}PROM) or Electrically Erasable Programmable Read-Only Memory, is a non-volatile storage chip used in computers and other devices to store data,
SHA-1 Hash Codes	The SHA hash functions are five cryptographic hash functions designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. SHA stands for Secure Hash Algorithm. Hash algorithms compute a fixed-length digital representation (known as a *message digest*) of an input data sequence (the *message*) of any length. They are called “secure” when (in the words of the standard), “it is computationally infeasible to: find a message that corresponds to a given message digest, or find two different messages that produce the same message digest. Any change

Abbreviation	Description
	to a message will, with a very high probability, result in a different message digest.
Software	Computer software is a general term used to describe a collection of computer programs, procedures and documentation that perform some task on a computer system. [1] The term includes application software such as voting servers which perform productive tasks for users, system software such as operating systems, which interface with hardware to provide the necessary services for application software.
PCMCIA Memory Cards:	Memory devices; also referred to as PC Cards
Voting System Components	The units of equipment (server platform, voting terminal, ballot scan device) when used together create a voting system
L&A	Logic and Accuracy testing; performed by the counties to assure the voting systems are functioning correctly
DRE	Direct-Recording Electronic touch screen
Scanner	Electronic scanner used to scan paper ballots
Central Count	Scanner configuration for batch processing of paper ballots where one or more scanners are directly linked to GEMS server and results are loaded in real time.
Precinct Count	Scanner configuration for processing of paper ballots where results are recorded on the AccuVote Memory card.
VVPAT	Voter Verified Paper Audit Trail.
EMS	Election Management System
TDP	Typical Data Package – contains all files, source code documentation produced for use during the certification process.
BOE	Board of Elections

7. ATTACHMENT A - COUNTY SURVEY

Questionnaire Instructions

The purpose of this questionnaire is to gather information regarding county-level practices to be used to in assessing the risk and vulnerability of voting systems to potential threats in a “real world” versus laboratory context.

The information you provide will be used to evaluate the effectiveness of your local security practices as countermeasures to vulnerabilities that may be identified in Red Team and technical testing activities as part of the State of Ohio’s Voting Systems Risk Assessment Study.

Because of the importance of local countermeasures, facilities and procedures in protecting voting systems from fraud and tampering, your complete, thoughtful and candid responses are critical to a comprehensive assessment of the actual risk facing your voting system(s).

The questions in this survey are intentionally open ended to permit you to respond appropriately to your own situation and practices. Please respond to each question (or set of questions) on separate sheets or pages. Please refer to the section and question as part of the response by either restating the question at the beginning of the response –or- by identifying the section and question by number.

In responding to the questions, please assume our familiarity with election concepts and terminology. In other words, it is not necessary to educate the audience on election processes or technology as part of your responses. In addition to describing your practices, we are interested in understanding the security related issues and constraints you face.

We realize that the completion of this survey will require the investment of several hours by key persons during an already busy time. Nevertheless, we ask that this survey be completed to the fullest extent possible by the appropriate person(s) and returned NO LATER THAN October 15, 2007.

Responses may be in electronic or hard copy format or both. Electronic responses should be sent to the email addresses below. Hard copy responses or documentation should be sent to:

Hugh Gallagher

Managing Director, ESAMS

6012 Glen Abbey Dr

Richmond, VA 23059

You will be contacted for an interview and site visit to review your responses, clarify any questions and address any gaps. You may be asked to provide a tour of your facility as part of your response.

Thank you for your assistance and cooperation.

Please contact SysTest Labs team members Hugh Gallagher, electionservices@aol.com or Scott Konopasek, Scott@forefrontelections.com if you need assistance or have questions regarding this survey.

County:

Voting System(s):

Person Completing this Survey:

Phone Number:

Email:

Please respond to the following questions with as much detail as possible separate pages as needed to provide a complete response to each question. Please provide supporting documentation (written policies or procedures) where it exists and applies.

Physical Security

1. Where are the voting equipment stored (DRE, ballot marking machines, precinct scanners, central count scanners, servers, election management/ballot layout workstations)? In what configuration? What security measures and access controls are in place at the storage facility(ies)? Please provide a sketch and description of the facility.

2. If an alarm or intrusion detection system is employed, please describe how it is used. Please provide a diagram depicting each sensor. Who manages the system? Where does the system alarm if an intrusion is detected? Who is notified? What are the response procedures?

3. How did you develop your physical security program (vendor instructions, state program and specific requirements or used county experience and expertise, etc)?

4. What is the strongest/most effective aspect of your physical security program? Why? What is the weakest/most vulnerable aspect? Why?

5. What resources are you lacking (be specific- guidelines, standards, budgetary, staffing levels etc.) in creating or managing your physical security program?

Access Controls

1. Is a badge system in place? Are photo badges used? Do the badges employ magnetic or electronic access control features? Who manages the badge system?

2. Describe access control procedures for sensitive areas for employees, temps, vendors and guests/observers. Please provide a list, by position, of who has access to which areas and equipment components. Describe how passwords and logon are used to control access.

3. Are background checks used in the hiring process? Who/ what positions are subject to background checks? What is checked and by which agency? What are disqualifying results?

4. How did you develop your access controls (vendor instructions, state program and specific requirements or used county experience and expertise, etc)?

5. What is the strongest/most effective aspect of your access control program? Why? What is the weakest/most vulnerable aspect? Why?

6. What resources are you lacking (be specific- guidelines, standards, budgetary, staffing levels etc.) in creating or managing your access control program?

Testing

1. Please briefly describe your election specific equipment and programming testing methodology, procedures and protocols for each voting system component (attach any written procedures). Include who performs the testing, where it is conducted, the scope of the testing and the timing/duration of the testing. Provide copies of written checklists.

2. How is the testing documented? Who signs-off or approves the results of the testing?

3. How and where is equipment or software secured after testing?

4. How did you develop your testing methodology and procedures (vendor instructions, state program and specific requirements or used county experience and expertise, etc)?

5. What is the strongest/most effective aspect of your testing program? Why? What is the weakest/most vulnerable aspect? Why? What is not tested that should be? Why?

6. What resources are you lacking (be specific- guidelines, standards, budgetary, staffing levels etc.) in conducting system testing program?

<u>Chain of Custody and Inventory Controls</u>

1. What controls and inventories are in place to account for and safeguard voting equipment (including electronic media) on an ongoing basis? Is an automated inventory control system used?

2. Please describe the inventory controls/ chain of custody for equipment that has been programmed, tested and/or prepared for an election: prior to delivery, during delivery, at the poll site prior to election day, when the polls are opened, during election day, when the polls are closed, while the equipment is being returned and when the equipment is received after the election.

3. How did you develop your chain of custody and inventory procedures (vendor instructions, state program and specific requirements or used county experience and expertise, etc)?

4. What is the strongest/most effective aspect of your chain of custody and inventory procedures? Why? What is the weakest/most vulnerable aspect? Why?

5. What resources are you lacking (be specific- guidelines, standards, budgetary, staffing levels etc.) in conducting effective chain of custody and inventory procedures?

<u>Other Security Measures</u>

1. In addition to the measures above, what security procedures or practices do you employ?

2. What do you think is the overall effectiveness of your security programs? Why?

3. What role does, or should, the Board of Elections play in developing and managing security requirements?

4. What role does, or should, the Secretary of State play in developing and managing security requirements?

5. What role does, or should, the voting system vendor play in developing and managing security requirements?

6. What is your level of confidence that your security procedures and measures are effective in countering any risks or vulnerabilities in the design or software of your voting system(s)? Why?

8. ATTACHMENT B - INTERVIEW GUIDE

1 Pre-Election Storage

- Intrusion Detection Systems (IDS) (non-working hours):
  - What area(s) protected
  - What types of sensors (access points, motion, video etc)
  - How monitored
  - How activated/armed
  - Alarm responses
- Access controls (working hours)
  - What area(s) controlled?
  - Type of controls
  - Levels of access
  - Enforcement practices
- Facilities
  - Designated secure areas
  - Access points
  - Layout
  - Door/wall construction
  - Ceilings
  - Back up power
  - Fire suppression
- Sensitive media
  - Verification of Software/firmware masters
  - Storage of Software/firmware masters
  - Logs/records for software/firmware
  - Maintenance/storage of individual memory cards
  - Labeling of sensitive media
  - VVPAT rolls
  - Voted ballots
  - Un-voted ballots

2 State 2: Election Preparation & Setup

- Election data maintenance
  - System of record
  - Parallel maintenance
  - Data cut off
- Data import, validation, proofing
  - What data
  - What systems
  - When
  - How validated
- Ballot Layout process
  - Who and when
  - What system(s)
  - Parallel layout (double data entry)
- Ballot proofing
  - Who and when
  - How
  - Sign off procedure
  - Audio
- Database setup
  - Who and when
  - How many db

  - Interfaces
- Database proofing
  - Who and when
  - How
- Bi-lingual ballots and proofing
  - Who and when
  - How
- Machine testing/maintenance
  - Who and when
  - What
  - Vendor role and support
- Machine programming
  - Who and when
  - What
  - Vendor role and support
  - Testing
  - Peripherals
- Logic and accuracy
  - Paper ballot methodology
  - DRE/ballot marking methodology
  - Audio ballot methodology
  - Public notice and participation
  - Observers

3 **State 3: Election Deployment of voting units.**

- Post testing
  - Application of seals/locks
  - Serial numbers
  - Serial logs and procedures
  - Other tamper indicating measures
  - Staging
- Delivery
  - Who and when
  - What
  - To whom and where
  - Vetting or bonding
  - Inventory controls
  - Logs and chain of custody

- Storage
  - Physical security
  - Accountability
  - Point of contact

4 **State 4: Polling Location Setup (Opening Polls)**

- Security checks
  - Tamper indicating procedures
  - Immediate actions
  - Reporting procedures
  - Zero report verification
- Site layout
  - Privacy considerations
  - Security considerations

5 **State 5: Voting Operations**

- Machine malfunctions

    - Immediate actions
    - Reporting
    - Paper jams/printer issues
    - Repair/recovery
    - Field personnel
    - Vendor role
- Machine tampering/electioneering
    - Voter misbehavior
    - Immediate actions
    - Reporting procedure
- Contingency/emergency plans
    - Missing/damaged equipment
    - Emergency situations
    - Natural disasters

6 **State 6: Voting Shutdown (Closing Polls)**

- Closing protocol
    - Tasks performed
    - Equipment/supplies returned
- Accountability
    - Unused ballots
    - Voted ballots by type
    - Electronic machines
    - Memory cartridges
    - Ballot Statement /Accountability forms
    - Chain of custody

7 **State 7**: **Election Data Transport**

- Packaging
    - Container
    - Paperwork
    - Seals
    - Identifying info
- Security
    - Who and how many transport
    - Delivery locations
    - Central location
- Chain of custody
    - Check in procedure(s)
    - Logs and records
    - Receipts
    - Resolving issues

8 State 8: **Election Results and Post Election Storage**

- Canvassing (Voters to ballots)
    - Absentee ballots
    - Provisional ballots
    - DRE ballots
- Reconciliation (Ballots cast to ballots reported)
    - How identified
    - Research tools and protocols
    - Resolution process
- Auditing (Votes cast to votes reported)
    - Type and scope of audits

    - Triggering events
    - Parallel monitoring
- Certification & Abstracts
    - Process
    - Reporting
- Recounts
    - Roles and responsibilities
    - Random selection process
    - Manual count procedure
    - Observer guidelines
    - Certification of recount

9. ATTACHMENT C – STUDY LIMITATIONS/CONSTRAINTS

Issue	Date Opened	Date Closed	Impact
Two week delay	09/11/07	9/24/2007	Expectations such as setup for the systems orientation and receiving documentation; causing an actual 4 week delay
Printed Documentation for each voting system and component	09/11/07	10/23/07	Slowed progress –document packages that were delivered were missing critical areas. A week lost for each system.
Premier DRE hardware not included	9/18/07	9/30/07	Week lost of testing ability
Passwords for Hart servers, laptops, BOSS and SERVO system	9/20/07	9/24/07	Two days lost of testing ability
Hart equipment missing from inventory	9/20/07	9/30/07	Week lost testing ability
Hart VVPAT paper missing in inventory	9/20/07	9/30/07	Setup and testing time lost – VVPAT paper was found to be in the Hart inventory room at the SOCC
ES&S Modem cable missing from inventory	9/20/07	10/2/07	Nine days testing time lost
Counties did not complete and return Questionnaire	9/11/07	11/26/07	Critical loss to report completion
Dayton Legal Blank was to print ballots and deliver election definitions as hired by the SOS to save time due to lost time in the beginning	10/26/07	12/07/07	Caused critical loss to capacity and ballot complexity testing.
SysTest Labs ES&S expert's time taken to answer SOS questions	11/16/07	11/16/07	A half day lost at a critical time period

Table 21 Capacity Testing Matrix Constraints

Manufacturer	DRE	% of Capacity	Optical Scanner	% of Capacity	Election Definition
Premier	TSx	100%	Accuvote Scanner	100%	Ohio Famous Names; SysTest Labs Creation; Dayton Legal Blank
ES&S	iVotronic	*	M100	81%	Ohio Famous Names ***
ES&S			M650	100%	Ohio Famous

	▨	▨			Names ***
Hart	eSlate	100%	eScan	**	2 - SysTest Labs Creations

* Unable to complete this portion of the test. ES&S would not provide information or support required to complete capacity testing
** The eScan requires unique ballots, i.e., once a ballot has been scanned, controls within the Hart System do not allow it to be scanned a second time. This required an inordinate number of unique ballots. The SOS requested that Dayton Legal Blank provide these ballots. Dayton Legal Blank did not provide the required ballots.
*** Complicated ballot layout test ballots required to be delivered by Dayton Legal Blank were not provided.

End of Report