

**Project**

**E V E R E S T**

**Evaluation and Validation of Election Related Equipment,  
Standards and Testing**

*REPORT OF FINDINGS*

OHIO SECRETARY OF STATE  
JENNIFER L. BRUNNER

COLUMBUS, OHIO  
DECEMBER 14, 2007



**Project EVEREST (Evaluation & Validation of Election-Related  
Equipment, Standards, & Testing)**

**Risk Assessment Study of Ohio Voting Systems**

**Executive Report  
Ohio Secretary of State Jennifer Brunner  
December 14, 2007**

## Table of Contents

<b>INTRODUCTION.....</b>	<b>5</b>
<b>OBJECTIVES.....</b>	<b>6</b>
<b>HISTORY .....</b>	<b>7</b>
OHIO'S PURCHASE OF ELECTRONIC VOTING MACHINES .....	7
PUBLIC CONFIDENCE IN ELECTRONIC VOTING.....	7
PROJECT EVEREST .....	8
<b>STRUCTURE OF STUDY .....</b>	<b>12</b>
<b>SECURITY ASSESSMENT .....</b>	<b>14</b>
MICROSOLVED .....	14
Method.....	14
Findings .....	15
Summary.....	15
Penetration Testing: Specific Results .....	16
<i>Premier</i> .....	16
Description of the Premier System.....	16
Physical Access Testing.....	20
Network and Communications Access Testing.....	22
File Systems Access Testing.....	22
Baseline Comparison .....	22
<i>ES&amp;S</i> .....	22
Description of the ES&S Voting System.....	22
Physical Access Testing.....	26
Network and Communications Access Testing.....	27
File Systems Access Testing.....	28
Baseline Comparison .....	28
<i>Hart InterCivic</i> .....	28
Description of the Hart InterCivic Voting System .....	28
Physical Access Testing.....	31
Network and Communications Access Testing.....	32
File Systems Access Testing.....	32
Baseline Comparison .....	32
Suggested Improvements: All Voting Systems.....	32
Summary of Boards of Elections Officials' Review of MicroSolved's Findings on the Security Assessment of the State's Voting Systems .....	33
UNIVERSITY RESEARCH TEAMS .....	35
Method.....	35
Findings .....	37
Summary.....	37
Specific Results: Source Code Analysis and Red Team (Penetration) Testing ....	38
<i>ES&amp;S</i> .....	38
Failure to Protect Election Data and Software.....	38
Failure to Effectively Control Access to Election Operations.....	39
Failure to Correctly Implement Security Mechanisms.....	40
Failure to Follow Standard Software and Security Engineering Practices ...	40

<i>Premier</i> .....	40
Failure To Effectively Protect Vote Integrity and Privacy/Failure to Protect Elections From Malicious Insiders .....	41
Failure to Validate and Protect Software / Failure to Follow Standard Software and Security Engineering Practices .....	42
Failure to Provide Trustworthy Auditing .....	42
<i>Hart</i> .....	42
Failure To Effectively Protect Election Data Integrity.....	43
Failure To Eliminate Or Document Unsafe Functionality .....	44
Failure To Protect Election From “Malicious Insiders” .....	44
Failure To Provide Trustworthy Auditing .....	44
Summary of Boards of Elections Officials’ Review of the Academic Research Teams’ Findings on the Security Assessment of the State’s Voting Systems.....	44
<b>CONFIGURATION MANAGEMENT ASSESSMENT.....</b>	<b>48</b>
SYSTEST .....	48
Method.....	48
Findings .....	49
Summary.....	49
Configuration Management Assessment: .....	49
Specific Results and Suggested Improvements.....	49
<i>Hart InterCivic</i> .....	49
<i>ES&amp;S</i> .....	50
<i>Premier</i> .....	51
Summary of Board of Elections Officials’ Review of SysTest’s Findings on Configuration Management of the State’s Voting Systems.....	52
<b>PERFORMANCE TESTING.....</b>	<b>54</b>
SYSTEST .....	54
Method.....	54
Findings .....	55
Summary.....	55
Performance Assessment: .....	56
Specific Results and Suggested Improvements.....	56
<i>Premier</i> .....	56
<i>ES&amp;S</i> .....	57
<i>Hart InterCivic</i> .....	60
Summary of Board of Elections Officials’ Review of SysTest’s Findings on Performance Testing of the State’s Voting Systems .....	61
Average Performance Report Quality Ratings by Election Officials .....	62
<b>ELECTIONS OPERATIONS AND INTERNAL CONTROL ASSESSMENT .....</b>	<b>63</b>
SYSTEST .....	63
Method.....	63
Findings .....	63
Summary.....	63
Specific Results and Suggested Improvements.....	64
Documentation.....	64
Threat Analysis.....	65
Vulnerability Analysis .....	66

Election Management Software (EMS) and Firmware Version Control Updates .....68

Summary of Boards of Elections Officials’ Review of SysTest’s Findings on the  
Elections Operations and Internal Controls Assessment of the State’s Voting  
Systems ..... 71

Average Operational Controls Report Quality Ratings by Election Officials.... 72

**SECRETARY OF STATE RECOMMENDATIONS ..... 73**

GENERAL CONCLUSIONS AND BACKGROUND ..... 73

RECOMMENDATIONS ..... 76

CONCLUSION .....84

## **Introduction**

Project EVEREST (Evaluation and Validation of Election Related Equipment, Standards and Testing) is a risk assessment of Ohio's current voting system, examining the integrity, handling, and securing of voting machines and systems before, during and after an election. The Ohio secretary of state has conducted this assessment in an effort to provide to the citizens of Ohio a comprehensive, independent, balanced and objective assessment of the accuracy, reliability and security associated with Ohio's voting systems.

The following is a summary of the Executive Report's sections:

- **Objectives** - The Objectives Section describes the overall objectives of the risk assessment study.
- **History** – The History Section summarizes the history of electronic voting in Ohio, and the impetus for and history of Project EVEREST.
- **Structure of Study** – The Structure of Study section describes the parallel testing design used in the study, which allows different parties to test the voting systems using multiple methods. This section summarizes the four tasks used to evaluate each system: security assessment, configuration management, performance testing, and operational controls.
- **Methods/Findings** – The Methods/Findings Section summarizes the methods used by each assessment team, and includes evaluation of the testing reports by a bi-partisan group of election officials, along with the findings reached using each method of assessment. This section is organized by the four tasks used to evaluate each system: security assessment, configuration management, performance testing, and operational controls.
- **Recommendations** – The Recommendations Section contains Secretary of State Jennifer Brunner's recommendations for how Ohio should best proceed in response to the declared findings, including long-term goals, short-term fixes, desired legislation and necessary secretary of state directives.
- **Appendices** – The Appendices Section includes the original Request for Proposals (RFP), State Controlling Board request, information regarding the boards of elections participants, all final testing reports, and a glossary of relevant technical terms.

## **Objectives**

The ultimate objective of Project EVEREST is to improve the integrity of Ohio elections for federal office, and state and local offices and issues, and provide the citizenry with increased confidence and trust in our elections system.

Project EVEREST has sought to accomplish these goals by attempting to provide a comprehensive, independent, balanced and objective assessment of the risks to election integrity associated with Ohio's voting systems, which will in turn be used to make improvements in laws and instructions governing Ohio elections with a focus on the use, handling, and securing of voting machines before, during and after elections.

In order to achieve these objectives, the following questions will be specifically addressed:

1. What are the significant risks of inaccuracy of election results, if any, due to error or fraud, including vulnerability to an "attack"<sup>1</sup>?
2. What are the significant risks of accidental or intentional catastrophic machine failure or unrecoverable error, if any?
3. Do risks exist that cannot be sufficiently mitigated, indicating inherent system inadequacies?

---

<sup>1</sup> An "attack" is a common term used when evaluating the security of a system and generally means an outside influence that may affect the operational integrity of the system.

## **History**

### Ohio's Purchase of Electronic Voting Machines

In 2002, the United States Congress adopted the Help America Vote Act of 2002 (HAVA), which aimed to improve the administration of elections in the United States. With the enactment of HAVA, new voting system requirements were established, and a national program was implemented to provide states with the funds necessary to replace punch card and lever voting systems with new, qualifying systems.

HAVA also created the U.S. Election Assistance Commission (EAC) and transferred the responsibility of developing voting system standards from the Federal Election Commission (FEC) to the EAC. Through HAVA, the EAC was also tasked with establishing the federal government's first voting system certification program.

Before the implementation of HAVA, the vast majority of counties in Ohio used punch card voting systems. With the advent of HAVA, voting machine manufacturers whose new systems met the applicable federal standards and whose equipment was approved for use in Ohio by the state's Board of Voting Machine Examiners<sup>2</sup>, submitted bids for consideration to the Ohio secretary of state. The secretary of state, in turn, worked with each county's board of elections (BOE) to purchase an approved system — either a direct recording electronic (DRE) or an optical scan system manufactured by Diebold (now Premier Elections Solutions), Hart InterCivic, or Election Systems and Software (ES&S) — that best-suited each particular county.

In May 2004, the General Assembly enacted Substitute House Bill 262, which required all DRE voting machines to provide a voter verified paper audit trail (VVPAT). The approved systems, with VVPAT, were subjected to an Independent Verification and Validation (IV&V) test and a security assessment performed by CompuWare. (The 2004 CompuWare study report may be found in Appendix A.)

Approximately half of Ohio's 88 counties used their new voting systems in the November 2005 general election; the other half used their new systems for the first time in the May 2006 primary election.

### Public Confidence in Electronic Voting

The response to the new voting systems has been varied, but overall, public confidence in the new machines and trust in Ohio's elections system have suffered. Individuals, election officials, non-partisan voting rights advocacy groups, and expert researchers both in Ohio and throughout the United States have expressed concerns regarding election integrity, security, accuracy, vote verification, and recounts using the various voting system technologies. Numerous documented malfunctions with elections systems and software, both statewide and nationally, have fueled public concern and contributed to the overall uncertainty of voters.

---

<sup>2</sup> See, R.C. 3506.05 *et.seq.* consisting of three persons appointed by the secretary of state, one of whom is a competent and experienced election official and the other two of whom are knowledgeable about the operation of voting equipment.



Other factors have contributed to the atmosphere of public uncertainty. Potential conflicts of interest in voting system certification, by which vendors select and pay testing labs to certify that their voting systems meet the system standards, have drawn much public scrutiny, as have questions surrounding the adequacy and timeliness of the federal certification and testing process. Another occurrence that has contributed to public unease is the failure of Ciber, Inc. to achieve accreditation by the U.S. Election Assistance Commission, long after Ciber's labs contributed to the certification of more than half of all nationally qualified voting systems. The EAC first temporarily barred Ciber from testing new machines in the summer of 2006 for failure to follow appropriate quality-control procedures and an inability to document that it was conducting all required tests.<sup>3</sup> More recently, the EAC voted to reject altogether Ciber's application to be a security test laboratory for electronic voting machines.<sup>4</sup>

Additionally, voting systems have recently been tested in several other states including California, Florida, New Jersey and Connecticut, all exposing serious flaws in the security of voting systems used in these jurisdictions, several of which are used in Ohio. California's testing resulted in the de-certification on a conditional basis of several components of its various voting systems. For these and other reasons, there is at least some doubt about the integrity of the state's election process and voting systems, and hence Project EVEREST was conceived, developed and implemented.

All public doubt and concern aside, technology is constantly evolving. Even if a voting system was certified under the most rigorous of certification standards, it is reasonable for the public to expect continued testing measures to ensure that voting systems safely, securely and accurately count their votes. Additionally, according to R.C. 3506.05(E), the secretary of state is statutorily required to "periodically examine, test, and inspect certified equipment to determine continued compliance."

### Project EVEREST

Project EVEREST was initiated by the secretary of state of Ohio to provide a comprehensive, independent, balanced, and objective assessment of the risks to election integrity associated with Ohio's voting systems, election-related equipment, testing, standards, and associated internal controls, including the extent to which integrity violations are possible, preventable, detectable, and correctable. The analysis was designed to assess the adequacy of institutional mechanisms of control and accountability as well as the ability to identify sources of error or potential fraud. Project EVEREST is designed as a risk assessment study of Ohio's voting systems' vulnerabilities and potential to mitigate them, providing a comprehensive analysis of the state's voting system as a whole.

Project EVEREST builds on other states' testing, by not only performing a wider range of testing in a secure laboratory environment, but by attempting to incorporate operational procedures used by election officials that could potentially mitigate security threats.

---

<sup>3</sup> Christopher Drew, "U.S. Bars Lab From Testing Electronic Voting," *The New York Times*, January 4, 2007.

<sup>4</sup> U.S. Election Assistance Commission, "Rejected Applications," Election Assistance Commission, <http://www.eac.gov/voting%20systems/test-lab-accreditation/interim-accreditation/pending-applications/?searchterm=ciber>

Project EVEREST's concept is unique in that it integrates the involvement of a bi-partisan group of election officials from a diverse selection of Ohio counties and voting machine environments to review the security assessments' applications to "real world" Election Day experiences.

After several months of research and planning, on June 18, 2007, the Ohio secretary of state issued a Request for Proposals (RFP) for consulting and testing services to perform the Risk Assessment Study of Ohio Voting Systems. The RFP outlines tasks to be performed and permitted proposers to submit proposals to perform one, some or all tasks. (The RFP may be found in Appendix B.) This allowed the secretary of state to select a combination of proposals to ensure all necessary tasks were performed to an optimal level and to facilitate a model of "parallel independent testing" of the state's voting equipment. Several entities representing corporate, professional and academic backgrounds were selected to execute the various tasks for accomplishing the project's objectives, and to provide unbiased, expert work from a diversity of corporate and academic environments.

On September 24, 2007, the State of Ohio Controlling Board approved the Ohio secretary of state's request to waive competitive selection, permitting these contracts to be awarded to SysTest Labs and MicroSolved, Inc. (The Controlling Board materials may be found in Appendix C.)

SysTest Labs, of Denver, Colorado, was selected to assess configuration management, operational controls and performance testing on each of the three certified voting systems in Ohio. SysTest is an approved test lab by the National Institute of Standards and Testing (NIST), and is an EAC federally approved Voting System Testing Lab (VSTL), offering Independent Verification and Validation (IV&V), Software Test Engineering, Quality Assurance (QA), and Compliance Testing services.

MicroSolved, Inc., of Columbus, Ohio, was selected to complete a security assessment of each voting system, evaluating vulnerabilities of each system by performing penetration testing. MicroSolved has performed past vulnerability assessments on sensitive networks found in the private sector and in state and federal government.

The project's academic teams were subcontracted through SysTest, to perform a variety of assessments in addition to and independently parallel to those mentioned above. The academics retained many individual researchers who are considered national and international experts in electronic security, with experience in evaluating security at the state and federal levels, as well as for the private sector, including highly sensitive federal and private sector projects. In addition to performing penetration testing, the project's academic teams performed a source code review of all three voting systems.

The Pennsylvania State University team was selected to perform penetration testing and source code analysis for the Hart InterCivic and Premier Election Solutions systems. In addition, the Penn State team was permitted by Premier to review unredacted reports of the state of California's "top-to-bottom" review of the Premier system to assist in its testing and analysis activities for the study.

The University of Pennsylvania team was selected to focus on the source code evaluation of the ES&S systems, with the potential to include penetration exercises or other security evaluation methods as deemed appropriate. In contrast, the University of California-

Santa Barbara WebWise team was chosen to focus on the penetration evaluation of the ES&S systems, with the potential to include source code analysis or other security evaluation methods as deemed appropriate.

Additionally, a project manager was engaged from Battelle Memorial Institute to provide project management services to the secretary of state's office for scientific oversight of the study schedule, contractor status, issue reporting and general project management.

All three voting machine manufacturers were actively involved in the voting system review. High-level executives from each manufacturer met with secretary of state staff at the beginning of the review to understand the project's operations and goals. All manufacturers pledged their support and cooperation at the outset of the project.

Each manufacturer sent at least one key staff person to conduct orientation on their respective systems. This orientation educated testers on machine operations, set-up, and breakdown.

The testing took place from October 5, 2007 through December 7, 2007. SysTest and MicroSolved's testing was performed under secure conditions at the State of Ohio Computer Center (SOCC) facility, and the three academic teams' testing was performed under secure conditions<sup>5</sup> at their respective universities.

To enable a real-world testing environment of voting equipment actually used in elections, several county boards of elections provided standardized and configured voting system equipment and software to the voting system review. Each voting machine manufacturer provided equipment to those respective county boards of elections to replace the equipment being tested. Additionally, each manufacturer supplied equipment that was unavailable from the county boards of elections. The manufacturers shipped the equipment free of charge.

The voting machine manufacturers also provided essential information to the voting system review. Computers were purchased for analysis of the "back office" for the voting system review to configure and tabulate ballots. The manufacturers configured and installed the necessary software on those computers and sent them to the SOCC to complete the test environments. They also provided the source codes necessary to analyze the voting system and critical confidential and proprietary documentation.

Additionally, the manufacturers provided ongoing support throughout the project. They answered technical questions and supplied documentation, equipment, and supplies such as VVPAT paper, ballots, and ballot stock. Throughout the project, manufacturers provided access to their high-level executives to answer questions and provide responses to testers' needs.

Upon the completion of the testing, SysTest, MicroSolved and the three academic teams provided to the Ohio secretary of state on or before December 7, 2007, their findings in various written reports. On December 9, 2007, the secretary, representatives from her administration, and the bi-partisan group of election officials convened to review and evaluate the various reports and used those findings to reach conclusions for the recommendations contained in this report.

---

<sup>5</sup> These secure conditions are based on industry standards according to uniform guidelines.

This Executive Report documents the cumulative results of the EVEREST assessment, and accordingly provides recommendations to the Ohio General Assembly and Governor Ted Strickland for improvements in laws and instructions governing Ohio elections with a focus on the use, handling, and securing of voting machines before, during and after elections. Both legislative and fiscal needs are detailed for the recommendations included in this report.

## **Structure of Study**

The Ohio Risk Assessment was designed to evaluate Ohio's voting systems along a multidimensional, layered approach so that independent perspectives could be compared for consistency. All voting systems approved for use in Ohio were evaluated under the four "tasks" of the project: (1) a security assessment; (2) a configuration management review; (3) performance testing; and (4) an analysis of the internal controls and operations associated with the voting systems. Upon conclusion of the review, all testing entities were required to submit both summary and detailed reports of their findings to the secretary of state. The secretary of state requested and received the assistance of a bipartisan group of county boards of elections officials who reviewed these reports and vetted and analyzed the recommendations made as a result of this study.

### **The Four Tasks of the Risk Assessment**

MicroSolved and the academic research teams were selected to conduct security assessments of each of Ohio's certified voting systems. Although the two testing entities utilized different methods, the goal of the parallel testing was to examine the security of the electronic voting systems in use in Ohio and identify procedures that may eliminate or mitigate discovered issues.

SysTest was selected to conduct the configuration management review, performance testing, and the analysis of operations and internal controls. Under the configuration management review, the goal was to evaluate the secretary of state's ability to independently verify whether the configuration of each voting system as approved for use by county boards of elections was consistent with, and unchanged from, the configuration certified by the state of Ohio, including, whether the certified configuration remained unchanged during all parts of the election process, including tabulation, during which results potentially could be affected. The purpose of the performance testing was to further determine if there were risks to the integrity of the election and accuracy of vote counts during simple use of each of the certified voting systems. Finally, the purpose of the elections operations and internal control assessment was to determine whether existing or proposed policies, procedures, and internal controls established in manufacturer documentation and administratively by and for county boards of elections are sufficient to ensure secure and accurate elections that may be affected by software, hardware, and operational susceptibilities.

### **Boards of Elections Officials' Review**

Along with the work of the testing entities, the Ohio Risk Assessment had the benefit of the efforts of an advisory group of Ohio boards of elections officials from twelve counties representing both major political parties in equal numbers. (A list of the boards of elections participants may be found at Appendix D.) During the testing of Ohio's voting systems, this group toured the secure testing facility and examined the machines tested and conferred during a weekly conference call with secretary of state team members to monitor project status. Upon conclusion of the testing, the group of election officials met for four days – from December 9, 2007 through December 12, 2007 – at the State of Ohio Computing Center in Columbus to review final reports and discuss with the secretary recommendations to be made as a result of the study.

While in Columbus, the boards of elections officials were first divided into five study groups, with each group tasked to review reports specific to a stated task of the study: (1) security assessment (MicroSolved); (2) security assessment (Academic research teams); (3) configuration management (SysTest); (4) performance testing (SysTest); and (5) internal controls and operations (SysTest). Each study group included at least two boards of elections officials (evenly distributed by party affiliation, except when there were three board officials to a team, and one team had one Republican and two Democrats, while the other had two Republicans and one Democrat) with each team staffed by three secretary of state employees — a “facilitator” to lead the group’s discussion, a “scribe” to document the group’s observations and conclusions, and an attorney for legal issues.

Each review team completed a questionnaire rating the testing entities’ reports in the following areas:

- The clarity of the problem and solution statements;
- The use of data to substantiate problems and solution statements;
- The logic and justifications used to argue from data to problems and solutions;
- The organization and readability of materials; and
- The overall quality of the work on a five-point scale of failing to excellent.

Reviewers were also encouraged to record relevant observations to support their ratings. Upon conclusion of the group’s review, the “scribe” created a “Capsule Summary Statement” of the group’s observations. This report contains those Capsule Summaries and a table of standardized findings according the criteria outlined above.

## Security Assessment

### MicroSolved

MicroSolved performed “red team” penetration tests of the Premier, ES&S and Hart InterCivic voting systems. MicroSolved attempted to “attack” the systems under a range of conditions – from that of a casual voter at a polling location to the skilled attacker with more direct access to the voting system. Unlike the Academic teams, MicroSolved was not given access to the voting machine manufacturers’ source code.

On all three voting systems, MicroSolved discovered “serious vulnerabilities in the systems and many of their components.” (Project Executive Summary Report at 2.) MicroSolved concluded: “[a]ll three vendor systems reviewed have serious gaps in compliance with even the most basic set of information security guidelines used by systems in industries such as finance, insurance, medical care, manufacturing, logistics and other global commerce. Given the extremely valuable data that these systems process and the fact that our very democracy and nation depend on the security of that data, much work remains to be done by all three vendors.” (Project Executive Summary Report at 12.)

MicroSolved created three reports for each voting system: (1) an Executive Summary Report; (2) a Technical Manager’s Report; and (3) a Technical Details Report. MicroSolved also created a Project Executive Summary Report. This Secretary’s Report briefly explains MicroSolved’s methods and findings. (The complete MicroSolved reports are attached at Appendix E.)

### Method

MicroSolved’s methodology followed a “traditional application assessment process,” which consisted of the following testing “phases”:

- **Attack surface mapping:** In the first phase, MicroSolved created a graphical representation of each voting system to determine the areas that were most likely available for assault by an “attacker.”
- **Threat modeling:** In the second phase, MicroSolved developed a model group of potential “attackers” – ranging from the casual external attacker to the focused/resourced internal attacker – and attempted to measure the extent to which these attackers could affect the confidentiality, integrity, and availability of any election or to simply introduce enough issues into the election process that the general public would fail to have confidence in an election.
- **Poor trust/cascading failure analysis:** In the third phase, MicroSolved examined the surface map of each voting system to identify areas where exploitation of vulnerabilities in the attack surfaces of components could lead to the introduction of malicious programming (malware) into the system – that is, where a security compromise could be spread from one component to another or from an external component to the core system.

- **Vulnerability assessment:** After identifying the potential attack surfaces in the previous phases, MicroSolved performed systemic testing of the voting systems to identify the presence of any security vulnerabilities. The vulnerability assessment emulated the “attackers” by performing testing appropriate for each group of “attackers” based on the various levels of access and capability.
- **Penetration testing and reporting:** The penetration phase – the most important of MicroSolved’s phases – explored the damage of exploiting the vulnerabilities identified in the vulnerability assessment. The penetration phase tested three types of access to each of the voting systems:
  - **Physical Access:** MicroSolved tested the system components for vulnerabilities through physical access, including probing the lock mechanisms, the accessible ports of the devices, and the input/output subsystems.
  - **Network and Communications Access:** MicroSolved tested the system components for networking and communications vulnerabilities, using network scanners, serial port probes, sniffing tools and exploit codes.
  - **File System Access:** MicroSolved tested the system components for vulnerabilities in the processing of elections data – that is, the way that the underlying operating system or applications interact with the file system.
- **Baseline comparison:** In order to compare the three voting systems against each other, the final phase of MicroSolved’s testing established a twelve-step framework of industry standard security best practices to “baseline” each system. MicroSolved assigned a “pass” or “fail” grade for each of the twelve requirements in the framework. “Passing” a category means that the voting system meets the best practices requirements for that area, and “failing” a category means that the system does not meet industry standard best practices.

## Findings

### Summary

MicroSolved’s review of the Premier, ES&S, and Hart voting systems identified three key weaknesses in each system.

- **First,** MicroSolved stated that the voting machine companies have “failed to adopt, implement and follow industry standard best practices in the development of the system.” Although basic best security practices have emerged over the previous ten years to assist organizations with the development, configuration, deployment, and management of IT infrastructures in a secure fashion, the three voting systems have failed to comply with these standards. (Project Executive Summary Report at 11.)
- **Second,** MicroSolved concluded there was a “lack of integrity controls” that have been applied to the voting systems. MicroSolved was able to identify



vulnerabilities in all three voting systems that could allow attackers to introduce an infection or malicious programming (malware) into the voting system. (*Id.*)

- **Third**, MicroSolved concluded that Ohio election officials have failed to establish or implement clear and effective security policies and processes, and because many county boards of elections face staff and budget shortfalls, the boards are prevented from having the resources to seek out security solutions on their own. (*Id.*)

### Penetration Testing: Specific Results

#### **Premier**

MicroSolved concluded that the Premier voting system performed “poorly” in the physical access and file system access penetration tests. However, the Premier system performed “well” in the network and communications access penetration test. (Technical Manager’s Report, Premier, at 10-11.)

#### Description of the Premier System

Premier voting systems are used in 48 Ohio counties – 47 counties utilize the Premier DRE as the primary voting machine, while one county uses Premier’s precinct count optical scanner as the primary voting system. To better understand the findings included in this report, the relevant components of the Premier system are described below.<sup>6</sup>

#### ***Components at County Boards of Elections Offices***

The following components reside at county boards of elections offices. The photographs are courtesy of the Academic research teams.

- **Global Election Management System (GEMS):** The GEMS server is responsible for running all election processes. Election officials use the GEMS server to create ballot definitions, program memory cards, and tally all votes after an election.

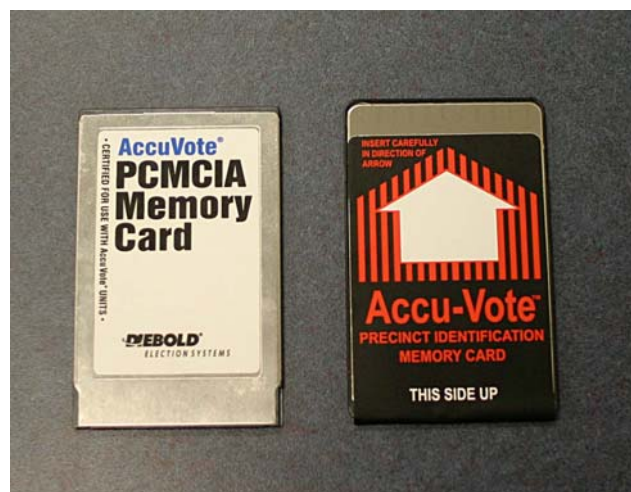
---

<sup>6</sup> Please refer to EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing, Final Report (hereinafter “Academic Final Report”) at Chapter 11, attached at Appendix F, for more detailed descriptions.



Premier GEMS Server

- Memory cards:** The Premier system relies on memory cards as the major avenue of communication between the GEMS server and the polling places. In counties using either DREs or optical scan machines, memory cards are encoded with ballot types at a board of elections office and sent to each polling place in the county for poll workers to configure the machines at the polling place. In some less populated counties, the DREs are delivered to the polling place with memory cards installed and with tamper-evident tape placed over each memory card to prevent its removal until the DRE is returned to the board or until the closing of the polling place. After polling places are closed, the ballots cast on either the DRE or optical scan voting machine are stored on the memory card, which is returned to the board of elections office and from which the GEMS server tallies the votes.



PCMCIA and AccuVote-OS Memory Cards used with the Premier Voting System

- **Election Media Processor (EMP):** The EMP is hardware and software used to communicate with GEMS and to interface with memory cards. Premier offers the EMP to efficiently encode and read memory cards. This device can read multiple memory cards in parallel.



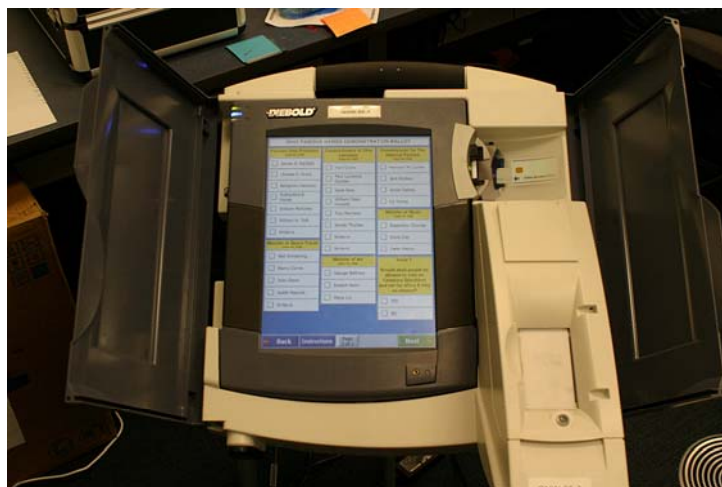
Election Media Processor (EMP) used with the Premier Voting System

- **Verdasys Digital Guardian:** Digital Guardian is additional third party software intended to enhance the security of the GEMS server. Because of previous security studies on the Premier voting system, the State of Ohio requires Premier to include the Digital Guardian software.

### ***Components at Polling Places***

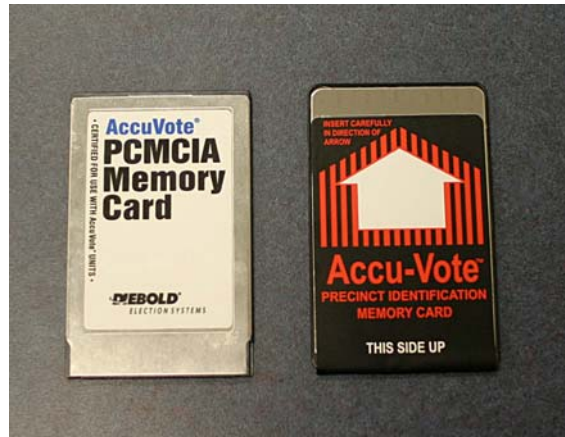
The following components are used at polling locations on Election Day.

- **AccuVote-TSX:** The TSX is a touchscreen DRE, which includes a VVPAT printer unit to create a verifiable paper record of the voter's selections.



Premier's AccuVote TSX DRE Voting Machine

- **PCMCIA Memory Cards:** See previous description of memory cards above.



PCMCIA Memory Card and AccuVote OS Memory Cards used with the Premier Voting System

- **Voter Access Cards and Supervisor Cards:** In counties using the TSX DRE machines, when a voter appears at a polling location to vote, the voter receives a Voter Access Card, which allows the voter to cast a single ballot. Upon reaching the TSX, the voter inserts the card into the machine and follows the on-screen instructions to cast a ballot. After the ballot has been cast and stored on the TSX and memory card, the TSX re-programs the Voter Access Card so that it cannot be used until re-encoded. Supervisor cards are given to the poll workers and are used to open and close the voting machines on Election Day.



Voter Access and Supervisor Cards used with the Premier DRE Voting System

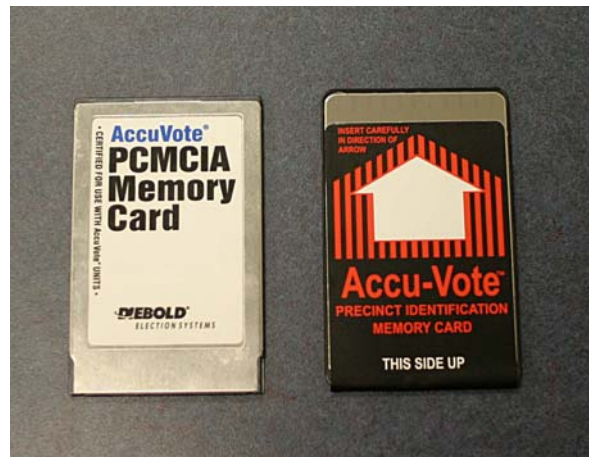
- **AccuVote OS:** The AV-OS Precinct Count is Premier's precinct optical scanner for use in each polling place or at a board of elections office. When a voter arrives at a polling place to vote, he or she marks an optical scan ballot with a marking device, such as a pen or pencil. When finished, the voter inserts the ballot into the AV-OS optical scan machine. The voter is given the chance to reject and retrieve the ballot (such as in the case of an overvote) or to accept the ballot as

voted. The ballots move from the scanner to a locked box in the base of the scanner. After the polling place closes, poll workers print an election summary off of the AV-OS. Poll workers transfer the AV-OS memory card, defined below, to the board of elections office for vote tabulating using EMPs and/or the GEMS server.



Premier's AccuVote Optical Scanner (AV-OS)

- AccuVote OS Memory Card:** On Election Day, AV-OS machines are configured by inserting memory cards that were encoded at the board of elections office. The AV-OS memory card stores the ballot images of the optical scan ballots scanned by the AV-OS on Election Day. After the polling place closes, poll workers transfer the AV-OS memory card to the board of elections office for vote tabulation.



PCMCIA Memory Card and AccuVote OS Memory Cards used with the Premier Voting System

### Physical Access Testing

Premier performed “poorly” in the physical access testing because MicroSolved was able to introduce malware into the system by various methods. MicroSolved concluded: “for devices whose intended deployments are to be public-facing and whose purpose is to

serve a critical function such as government elections, the systems seemed woefully inadequate from physical attacks.” (Technical Manager’s Report, Premier, at 12.)

MicroSolved described the following security vulnerabilities resulting from its physical access penetration testing:

- At the precinct level, locks on the optical scanners and ballot storage/sorting bins were “easily circumvented” using common lock picking tools. (*Id.* at 12.)
- The keys to the physical locks of several devices, including keys to DREs, are not unique and easily obtainable, which could expose many systems to tampering. (*Id.*)
- Physical attacks on the DRE unit were identified that would cause the unit to boot into administrative mode, in which an unauthorized individual could gain access to reconfigure the DRE device, change election settings, and delete electronic ballot results previously cast on the voting machine under the individual’s control. Additionally, security protections on the power button and primary memory slot could be “easily circumvented.” (*Id.*)
- The tamper seals on the DRE unit could be manipulated to make it appear as if tampering has occurred, even if tampering has not occurred. Threat agents working in teams could therefore create general chaos in the election process and disrupt public confidence in an election. (*Id.*)
- The GEMS server and connected EMP workstations that were operated at the board of elections’ offices were discovered to be “poorly configured” and “poorly protected against physical access attacks,” which could allow unauthorized individuals to deploy malware or other malicious code if given access to the system, even for a short period of time. (*Id.* at 13.) For example, the EMP workstations tested did not have anti-virus software installed, and the anti-virus software installed on the GEMS server had not been updated in approximately two years.
- The protections offered by the Digital Guardian security tool, a security program developed specifically for the GEMS server in Ohio and which is installed to overcome already known weaknesses publicly identified in other tests, are “easily circumvented.” (*Id.* at 13.) The Digital Guardian application is not configured to enforce many of the rules for which it is programmed. For example, instead of actually blocking user actions recognized as malicious, Digital Guardian simply alerts the user that the actions have been detected but allows the actions to occur.
- Password policies on the EMP workstations and GEMS server are not in compliance with industry standards and are vulnerable to simple attacks by deciphering the password. (*Id.* at 13-14.)
- Because the Premier system does not serialize optical scan ballots, the ballots are not unique, and optical scan ballots could be re-processed through the optical scanner a second time without notice. (*Id.* at 14.)

### **Network and Communications Access Testing**

The Premier system performed “well” in the network and communication access testing. Manipulation of the communications streams and network traffic failed to discover any significant vulnerabilities. (Technical Manager’s Report, Premier, at 11.) However, MicroSolved did discover weaknesses in the protection mechanisms installed on the GEMS server. For example, MicroSolved identified a vulnerability in the firewall software used to protect the GEMS that allows unauthorized individuals to exploit the GEMS server. As in the physical access testing, MicroSolved also identified poor password policies. These weaknesses expose the GEMS server to network compromise from the EMP workstation or other network devices by an unauthorized individual or malware. (*Id.* at 11, 14-15.)

### **File Systems Access Testing**

The Premier system performed “poorly” in the file systems testing. Several components were found to be vulnerable to input manipulation attacks that could introduce arbitrary code into the system. (Technical Manager’s Report, Premier, at 11, 15.) For example, MicroSolved was able to boot a DRE voting machine into administrative mode based on the data on a memory card inserted into the machine. MicroSolved also identified a “plethora” of buffer overflow exploits. (*Id.* at 15.) Buffer overflow occurs by writing outside the bounds of a block of allocated memory and can corrupt data, crash the program, or cause the execution of malicious code. (*Id.* at 21.) Finally, MicroSolved found ways that unauthorized individuals could manipulate files processed by the EMP workstations connected to the GEMS server at a board of elections to cause the server tabulating votes to report precincts having been counted but the votes from the precinct were not actually added to the tally of the results. (*Id.* at 16.)

### **Baseline Comparison**

Premier scored a “zero” on its twelve-step baseline comparison framework – that is, the Premier voting system failed to meet any of the twelve basic best practices requirements. (Technical Manager’s Report, Premier, at 17-19.)

### **ES&S**

MicroSolved concluded that the ES&S voting system performed “poorly” in the physical access and file system access testing. However, ES&S performed “medium” in the network and communications access testing. (Technical Manager’s Report, ES&S, at 9-10.)

### **Description of the ES&S Voting System**

ES&S voting systems are used in 39 Ohio counties – 11 counties utilize the ES&S DRE as the primary voting machine, while 28 counties use ES&S’s precinct count optical scanner as the primary voting machine. To better understand the findings included in this report, the relevant components of the ES&S system are described below.<sup>7</sup> The photographs are courtesy of the Academic research teams.

---

<sup>7</sup> Please refer to the Academic Final Report at Chapter 5, attached at Appendix F, for more detailed descriptions.

### ***Components at the Boards of Elections Offices***

The following components reside at county boards of elections offices.

- **Unity:** Unity is the election management software for the ES&S system and is responsible for running all elections processes. Unity is a suite of software that creates ballot definitions, programs memory cards, and tallies votes after an election.
- **Model 650:** The M650 is a centralized high-speed optical ballot scanner and counter intended for use at boards of elections offices.



ES&S Model 650 Central Count Optical Scanner

### ***Components at Polling Places***

The following components are used at polling locations on Election Day.

- **iVotronic:** The iVotronic is the DRE touchscreen voting machine. All iVotronic machines used in Ohio include a VVPAT printer unit, which creates a physical copy of a cast ballot on thermal paper. The VVPAT records individual touches on the screen, including changes in a vote but does not create a summary of a voter's ballot at the end of the voting process like the Premier TSX DRE does. Voter verification must occur as the voter votes on each selection.





ES&S iVotronic DRE Voting Machine

- Personalized Electronic Ballot (PEB):** The PEB is a palm-sized hardware token that also stores ballot definitions for and records election results from an iVotronic DRE voting machine. In counties using the iVotronic DRE as the primary voting machine, boards of elections load each PEB with ballot types. One PEB for each precinct is chosen as the master PEB, and the others are referred to as supervisor PEBs. On Election Day, the master PEB opens and closes each iVotronic DRE. When a voter arrives at a polling location to vote, a poll worker inserts his or her supervisor PEB containing the ballot images into the iVotronic. The poll worker then removes the supervisor PEB, and the voter votes. The vote is recorded internally in the iVotronic and in a compact flash memory card contained in each machine. When the polling place closes, a poll worker inserts the master PEB into each of the iVotronic DREs in the precinct so that the single master PEB can collect and store the votes for all DREs in the precinct. The flash cards from each machine and the master PEB from each precinct are then returned to the board of elections office for tabulating the votes.



ES&S Personalized Electronic Ballot (PEB) for the iVotronic DRE Voting Machine  
(compared to the size of a quarter coin)

- **Flash Memory Cards:** The flash memory cards are used for various iVotronic DRE election functions, including updating its software and recording votes. Before each election, a flash card is programmed and inserted into each iVotronic. After an election, the memory cards provide an additional way to tally votes.



Flash Memory Card for iVotronic DRE Voting Machine  
(compared to the size of a quarter coin)

- **Model 100:** The M100 is the ES&S precinct-based optical ballot scanner. Before an election, the M100 is programmed by a prepared PCMCIA memory card to allow the machine to read the polling location's ballots. When a voter arrives at the polling location to vote, the voter is given an optical scan ballot. After marking his or her selections on the optical scan ballot, the voter inserts the ballot into the M100 optical scanner. The voter is given the chance to reject and retrieve the ballot (such as in the case of an overvote) or accept the ballot as voted. The M100 keeps a running tally of votes internally and on a PCMCIA memory card. After the polling place closes, the PCMCIA card is removed and the locked ballot box contained in the base of the scanner is removed. The PCMCIA cards and the ballot boxes are transported to the board of elections office for tabulating the vote.



ES&S Model 100 Precinct Count Optical Scan Voting Machine

- **PCMCIA memory cards:** The M100 optical scan voting machines use PCMCIA flash storage memory cards encoded with ballot types from the Unity software operated at the board of elections office. Before an election, appropriately-encoded PCMCIA cards are inserted into an M100 to be used at a polling location. The M100 reads proper election definitions from the prepared

PCMCIA card when the ballot is scanned into the machine. After an election, the PCMCIA card is removed from the M100 at the precinct and transported to the board of elections office for tabulating the votes.



PCMCIA Memory Card for M100 Optical Scanner (compared to the size of a quarter)

- AutoMARK:** The AutoMARK is a combination scanner/printer used by a voter – typically a voter with disabilities. The AutoMark allows touchscreen voting but uses a pre-printed ballot that contains a bar code. When an unvoted ballot is inserted into an AutoMARK machine, the machine reads the ballot’s bar code and identifies the ballot type, allowing the voter to vote by touching the screen and marking the voter’s selections onto the blank ballot. When a voter finishes voting, the ballot is ejected as marked for the voter to place the ballot into a ballot box or to insert the voted ballot into an optical scan machine.

### Physical Access Testing

The ES&S system performed “poorly” in the physical access testing because physical access to many of the system components could be used to “cause availability issues,” making voting machines inoperable to “attack the integrity of the elections data and process and introduce chaos in the elections process.” (Technical Manager’s Report, ES&S, at 9.)

MicroSolved described the following security vulnerabilities resulting from its physical access penetration testing:

- At the precinct level, the Automark – an ES&S electronic ballot printing device that does not tabulate votes, but rather prints voter’s decisions on a pre-printed optical scan ballot – could be easily compromised to allow an unauthorized individual to introduce malware into the system and affect how ballots are marked. The effects of this attack, however, may be minimal, as a voter is able to visually detect any errors on the ballot prior to inserting the ballot in the optical scanner or submitting it for counting. Nonetheless, an attacker could introduce malware into the Automark that is transferred to a memory card that at some point is reloaded into the Unity server operated at the board of elections. (*Id.* at 10-11.)

- ES&S precinct optical scanner, the M100, is susceptible to attacks at the polling location that could affect election integrity. First, a simple physical manipulation of the machine could result in it performing its poll closing function. As a result, an unauthorized individual could delete records of votes by zeroing out the vote totals. Second, an unauthorized individual with physical access to memory cards could prevent some or all scanned ballots from being recorded to the memory card for an M100 optical scan machine. MicroSolved determined it “likely” that unless there is close scrutiny or a recount of the precinct using the paper tapes and the actual ballots for a machine, the attack would go undetected. (*Id.* at 11.)
- Physical battering of a DRE by a voter at the precinct could easily cause the voting machine to have to be rebooted, causing delays and confusion during the voting process. (*Id.* at 11.)
- At the board of elections level, there are “critical weaknesses” in the security configurations of the computers running the Unity software. (*Id.* at 11.) MicroSolved concluded: “the computers hosting the software failed to be secured from physical attack in even the basic ways,” and unauthorized individuals could leverage these security weaknesses to introduce malware or compromise elections data. (*Id.* at 11.)
- The server and workstation lacked proper password policies, anti-virus software, and basic mechanisms for managing the integrity and security of the system. (*Id.* at 11-12.)

### **Network and Communications Access Testing**

ES&S performed “slightly better” in the network and communications access phase of the penetration testing by scoring a “medium.” (*Id.* at 10, 12.) However, problems remained in the equipment used in the precincts and at boards of elections. MicroSolved identified the following security vulnerabilities in its network and communications access phase:

- The DRE units showed a vulnerability in the printer connection where unauthorized individuals could easily connect their own device to the VVPAT printer and print their own results or rewind the paper tape to print over the existing voter records. (*Id.* at 12.)
- At the board of elections office, network attacks against the Unity server’s Windows 2003 storage server and the Windows XP workstation proved possible, which would allow an unauthorized individual access to the server’s network to compromise election data. Lack of firewalls on the PC devices, poor password and configuration policies, and the availability of unneeded services contribute to the identified risk. MicroSolved concluded: “It would be easy for an attacker who gains network access to compromise one or both of the computers and introduce malware to the system to alter voting data over time or outright destroy the software.” (*Id.* at 12.)

### **File Systems Access Testing**

The ES&S system performed “poorly” under the file systems testing. Several vulnerabilities on system components used at precincts and boards of elections could be used to introduce malware to the components. (Technical Manager’s Report, ES&S, at 10, 12.) MicroSolved identified the following security weaknesses in the file system testing:

- At the precinct level, the interaction of the DRE units with their memory cards proved to be “extremely vulnerable.” (*Id.* at 12-13) MicroSolved was able to cause a DRE to crash by tampering with a memory card, which could cause an unauthorized individual to introduce malware into the DRE component or its memory card and transfer illicit code to the Unity server. While access to memory cards is protected with tamper seals, MicroSolved found the seals were “easily circumvented.” (*Id.* at 13.)
- At the board of elections level, more “critical vulnerabilities” were identified. (*Id.*) For example, “fuzzing” – a software testing technique that consists of finding implementation bugs using malformed data injection in an automated fashion – of a certain file of ES&S’s central count optical scan machine, the m650, caused errors in the tabulation mechanism, which could be used to manipulate the vote count in the tabulation process. The Unity software also showed several areas of exposure to file fuzzing and input formatting attacks. According to MicroSolved, “[b]y leveraging these vulnerabilities through either direct access or through malware, an attacker is likely to be able to damage the software or influence its proper operation and handling of vote data.” (*Id.*)
- By using simple network applications, MicroSolved was able to reveal sensitive data hard coded in the software. Unauthorized individuals could use this information to design malware or compromise the software. (*Id.*)
- A mechanism exists in the Unity software for a user to arbitrarily edit vote totals. (*Id.*)

### **Baseline Comparison**

ES&S scored a “one” on the twelve-step baseline comparison framework – that is, the ES&S voting system failed to meet eleven of the twelve basic best practices requirements. (*Id.* at 15-16.)

### **Hart InterCivic**

The Hart InterCivic voting system performed “poorly” in the physical access testing and the file system access testing. The system performed “intermediate” in the network and communications access testing. (Technical Manager’s Report, Hart, at 9-10.)

### **Description of the Hart InterCivic Voting System**

The Hart voting system used in Ohio is a combination of DRE and optical scan components and is used in 2 Ohio counties. To better understand the findings included

in this report, the relevant components of the Hart system are described below.<sup>8</sup> The photographs are courtesy of the Academic research teams.

### ***Components at County Boards of Elections Offices***

The following components reside at county board of elections offices.

- **BOSS:** The Ballot Origination Software Systems is the Hart software used to set up an election, including defining the ballot for each precinct. BOSS exports election data to MBBs, described below, which transport the ballot definitions to each polling location.
- **Tally:** Tally is the Hart software that tabulates the votes in an election. After polling places close, MBBs from each precinct are delivered to the board office and loaded into the server for Tally to tabulate and generate reports of the election results.



Hart Software

### ***Components at Polling Places***

The following components are used at polling locations on Election Day.

- **MBB:** A Mobile Ballot Box is a PCMCIA card that stores ballot definitions and vote results. MBBs are the primary means of transmitting election data between a polling place and the board of elections. Before an election, ballot definitions are transmitted from BOSS to an MBB. MBBs are then installed into the JBC, described below, and also into eScan devices, described below, and tamper-sealed into these machines. The MBBs may also be transported to the polling locations for installation onsite at each precinct. After polling places close, MBBs from the JBC and eScan units are transported back to the board of elections for tabulating votes.

---

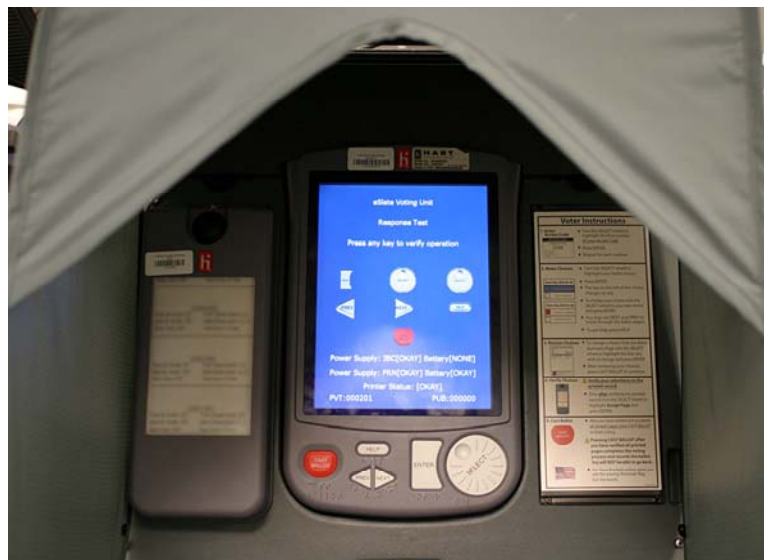
<sup>8</sup>Please refer to the Academic Final Report at Chapter 17, attached at Appendix F, for more detailed descriptions.

- JBC:** The Judge's Booth Controller is a console that controls access to all the Hart DREs (eSlates, described below) at a polling location. The JBC can be connected to up to twelve Hart DRE voting machines. The JBC generates voter access codes, distributes ballot configuration to the eSlates, records votes, and stores eSlate ballots to internal memory. MBBs are also inserted into a JBC to store ballots. On Election Day, poll workers start the JBC by entering a password. After an election, the MBBs from the JBC are transported to the board of elections for tabulating votes.



Judges Booth Controller for DRE eSlate Voting Machines

- eSlate:** The eSlate is a DRE voting unit used in a Hart-run precinct – typically for voters with disabilities. When a voter arrives at a polling location to vote on the eSlate, the voter proceeds to the poll worker staffing the JBC. Each voter receives a 4-digit access code. The voter proceeds to the eSlate where he or she enters the code and votes according to the instructions. At the close of the election, poll workers enter a password into the JBC to close the polls and the eSlate machines. The MBB from each JBC is transported to the board of elections for vote tabulation.



## Hart eSlate DRE Voting Machine

- eScan:** The eScan is Hart's precinct-based optical ballot scanner. The eScan scans and tabulates optical scan ballots and contains an MBB used to store tabulated vote results. Before an election, ballot definitions are transmitted to the eScan through an MBB. On Election Day, poll workers activate the eScan by entering a password. During an election, voters complete an optical scan ballot and insert it into the eScan machine. The voter is given the chance to reject and retrieve the ballot (such as in the case of an overvote) or accept the ballot as voted. After the polling places close, poll workers enter a password into the eScan to close the machines and prevent further voting. The MBB from the unit is transported to the board of elections for vote tabulation.



Hart eScan

### Physical Access Testing

The Hart system performed “poorly” in the physical access testing because physical access to the optical scanner device and the two computer systems hosting the Hart software was “tantamount to complete compromise of the system.” (Technical Manager’s Report, Hart, at 9.) MicroSolved identified the following security issues in the physical access testing:

- At the precinct level, the DRE voting units and Judges Booth Controller unit at the precinct level are “quite resistant to physical attack. . . . The team could not identify a way to circumvent the operating modes of these units or achieve access to their underlying operating systems.” (*Id.* at 11.)
- Physical attacks against the Judges Booth Controller led to the discovery of a potential problem with the generation of voter access cards, which could allow an unauthorized individual to vote multiple times using the DRE device. (*Id.*)
- Compromise of the precinct optical scanner can be “easily gained.” An unauthorized individual with sufficient knowledge could “easily overcome the tamper seals and either modify or replace the operating system files or memory card.” (*Id.*) Highly resourced individuals could then introduce malware that could affect the integrity of the election.



- The ballot box on the optical scanner was easily unlocked using common lock picking techniques, which would allow unauthorized individuals to access voted ballots. (*Id.* at 12.)
- The security of the PCMCIA memory cards used to carry the elections data between the precincts and the board of elections is “inadequate.” (*Id.* at 12.) Unauthorized individuals who gain access to the memory cards can easily tamper with the data and affect election integrity.
- At the board of elections level, both computers used with the Hart voting system were “easily compromised.” (*Id.*) Unauthorized individuals could “easily circumvent” any existing protections. (*Id.*)

### **Network and Communications Access Testing**

The Hart system performed “intermediate” during these tests because exploitation of the optical scanner was not proven possible. (*Id.* at 10.) However, MicroSolved identified the optical scanner as running insecure services. In addition, the network connection used to transfer elections data between software components was found to be improperly transferring data in text without encryption, and the computers hosting the software were found to be “easily compromised” through deciphering passwords. (*Id.*)

### **File Systems Access Testing**

The Hart system performed “poorly” in the file systems access testing because unauthorized individuals could gain access to the memory cards and “easily tamper” core voting data. (*Id.* at 10.) MicroSolved identified two critical risks:

- The database storing election data is unencrypted. Unauthorized individuals could therefore gain access to election data. Unless auditing is performed against the paper tapes, this would likely go undetected. (*Id.* at 13.)
- System software allows editing of election results. While editing is logged, the logs could be missed or deleted by an unauthorized individual. (*Id.*)

### **Baseline Comparison**

Hart scored a “zero” on the twelve-step baseline comparison framework – that is, the Hart InterCivic voting system failed to meet any of the twelve basic best practices requirements. (*Id.* at 14-16.)

### **Suggested Improvements: All Voting Systems**

MicroSolved reported three suggestions for improvement:

- **First**, all parties, including voting machine manufacturers, must “embrace industry standard best practices” and election officials must “enforce them through technology, policy and process and education.” (Project Executive Summary Report at 11.)

- **Second**, the voting manufacturers must proceed to “deploy proper integrity controls such as anti-virus software, firewalls, encryption and deeper techniques such as proper bounds checking on inputs and other security programming standards.” (*Id.*) Additionally, the secretary of state must implement use of the Digital Guardian security tool on all voting systems and ensure that the tool is correctly configured.
- **Third**, the voting machine manufacturers must “undertake a systemic approach to mitigating the identified vulnerabilities in the system.” (*Id.*) MicroSolved concluded: “Each issue mitigated by the vendor greatly reduces the amount of risk management that must be transferred to the counties by policy and process controls. Given the lack of resources many of the counties face, this is likely to have significant impact on the entire election process.” (Technical Manager’s Report, Premier, at 17.) The specific security vulnerabilities identified by MicroSolved are listed in its Technical Details Report for each system, which is attached at Appendix E.

### **Summary of Boards of Elections Officials’ Review of MicroSolved’s Findings on the Security Assessment of the State’s Voting Systems**

Two Republicans and one Democrat boards of elections officials reviewed MicroSolved’s findings on the security of Ohio’s three voting systems. All three of these officials utilize the Premier DRE voting system in their respective counties. In addition to the elections officials, the review group consisted of three secretary of state employees — a facilitator, an attorney, and a “scribe.” A “Capsule Summary Statement” of the elections officials’ review is provided below, basically as prepared by the “scribe,” along with a table summarizing this boards of elections review team’s standardized evaluation of MicroSolved’s findings.

#### **Capsule Summary Statement by Boards of Elections Teams Reviewing MicroSolved’s Findings**

##### **Executive Summary (All Systems): Group Summary Statement**

- The report is useful, but the summary table is vague. The report is useful in that it can start the conversation, but one does not know if the poll worker or any other unauthorized individual could emulate one of the security attacks. As election officials, we can now go back and re-evaluate what is being done in our office. However, we can see where some of these security attacks could happen — for instance, we can see where the use of generic log accounts allow unidentified users to access the Premier GEMS server.

##### **Premier Report: Summary Statement**

- The overriding theme in all of the MicroSolved reports is that Ohio needs to have statewide written procedures for security. Basic updates to Windows, such as patches certified from Windows, must be allowed without having to go through the Board of Voting Machine Examiners. The voting machine manufacturers must update the software or hardware for the voting systems.

While written procedures are needed in all 88 counties, the state needs to take into consideration that every board of elections is different. Statewide procedures should take into account that in one county there may be two employees, and only one may work on voting equipment or the server. In other counties, however, there may be many employees, and neither the Director or Deputy Director operates the voting equipment or server.

While gaining access to change vote totals is necessary and provided for in Ohio election law, there should be an audit log demonstrating when and if this occurs. Server software should not allow its databases to be opened through a Windows program without having the server software open.

The reports were very thorough, and brought up new topics to start the conversation.

### **ES&S Reports: Group Summary Statement**

- The boards of elections officials could relate to this report more than the Hart report. MicroSolved found more problems with the ES&S machines but clarified their statements and gave good explanations. The findings in the reports are “scary,” but the report is “very good.”

### **Hart Reports: Group Summary Statement**

- The group felt that the report gave good, quality answers, but the group did not feel that every hypothetical security attack was possible. However, the report presented a problem and a corresponding solution, which is what the boards of election officials were seeking.

### **Summary Table of Standardized Evaluations**

#### **Average Commercial Security Report Quality Ratings by Election Officials**

Quality	Scale	Executive Summary	ES&S	Hart	Premier
Data	1-3	2.3	2.7	2.3	3.0
Claims	1-3	2.3	2.7	2.3	2.3
Warrants	1-4	3.0	3.0	3.0	3.7
Coherence	1-4	3.7	4.0	3.7	4.0
Overall	1-5	4.3	4.7	4.3	4.3

Note. This table represents the average ratings of three election officials.

#### **Report Quality Rating Scales**

Scale	Dimension Measured
Data	Conclusions were based on and supported by data.
Claims	Claims were clear, consistent, feasible, and related to solutions
Warrants	Arguments were reliable, trustworthy, and logical
Coherence	Material was integrated and contained sufficient context
Overall	Overall report quality from failing to excellent

## University Research Teams

The Academic researchers performed source code analysis and “red-team” testing of the Premier, ES&S, and Hart voting systems. Because the ES&S voting system has not yet been the subject of a detailed security review, a team of faculty and graduate students at the University of Pennsylvania focused on a source code analysis of the ES&S voting system, and a collection of security consultants at Webwise Security, Inc., supported by two experts from the University of California at Santa Barbara, focused on the red-teaming exercises on the ES&S voting equipment. A team of faculty, graduate students, and one consultant at the Pennsylvania State University focused on the source code analysis and red team testing of the Hart and Premier voting systems. The Hart and Premier voting systems have been the subjects of previous security reviews conducted outside of the State of Ohio.

Parallel to MicroSolved’s review, the Academic research teams attempted to assess the security of the voting systems used in Ohio and identify procedures that may eliminate or mitigate discovered issues. The Academic teams concluded: “All of the studied systems possess critical security failures that render their technical controls insufficient to guarantee a trustworthy election.” (EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing, Final Report (hereinafter “Academic Final Report”) at 3.) Further, the researchers found that “such flaws mandate fundamental and broad reengineering before the technical protections can approach the goal of guaranteeing trustworthy elections.” (*Id.* at 4.)

The Academic teams created one Academic Final Report – consisting of 316 pages – outlining the methods and results of their review. The Academic Final Report is divided into five parts. Part I provides an executive overview of findings, a broad description of the evaluation structure – including a “threat model” used to structure the evaluation of voting machine security for all three systems – activities, and limitations, and it identifies the security features of the three voting systems. Parts 2 through 4 detail each voting systems’ evaluation. Part 5 contains reference appendices providing supporting technical and testing procedure information. Much of Part 5 is redacted in the Appendix to protect voting systems currently in use from being abused or penetrated. This Secretary’s Report briefly explains the Academic teams’ methods and findings. The complete Academic Report is attached at Appendix F.

### Method

The first step in the Academic security analysis was to define the “threat model.” Similar to that used by MicroSolved, the research teams’ threat model describes (1) the goals an “attacker” might have, (2) the types of attackers that might attempt to attack the system, and (3) the capabilities available to each type of attacker. (*Id.* at 11.)

- **Attacker Goals:** The researchers first identified the possible “attacker” goals:
  - Producing incorrect vote counts
  - Blocking some or all voters from voting
  - Casting doubt on the legitimacy of the election results

- Delaying the results of the election from becoming known, or
- Violating the secrecy of the ballot.
- **Potential Attackers:** The researchers' model then considered the following broad classes of attackers:
  - **Outsiders:** Outsiders have no special access to any voting equipment, other than attacks based on equipment connected to the internet or breaking into storage facilities to tamper with voting equipment.
  - **Voters:** Voters have limited and partially supervised access to voting systems during the process of casting their votes.
  - **Poll workers:** Poll workers have extensive access to polling place equipment, including management of the voting equipment, before, during, and after voting.
  - **Election officials:** Election officials have extensive access to the election management systems and the voting equipment. If election officials have unsupervised access to the systems, the integrity of those systems is provided purely by the integrity and honesty of the election officials.
  - **Vendor employees:** Vendor employees have access to the hardware and source code of the system during development and also assist election officials. Some vendors use third-party maintenance and Election Day support whose employees are not tightly regulated.
- **Types of Attacks:** The researchers categorized the severity of attacks along the following dimensions:
  - **Detectable vs. Undetectable:** Some attacks are undetectable, while others are detected in principle but unlikely to be detected unless certain election processes or procedures are routinely followed. An undetectable threat is especially severe and high priority, as the public could never be certain that the election results were not corrupted by undetected tampering.
  - **Recoverable vs. Unrecoverable:** If an attack is detected, there is often a way to recover. In contrast, some attacks can be detected, but there may be no good recovery strategy. Attacks that are detectable but not recoverable are serious, although not as serious as undetectable attacks. The researchers presumed that most elections will not be subject to attack, and the ability to verify that any particular election was not attacked is valuable.
  - **Prevention vs. Detection:** The researchers presumed that voting systems are designed as a tradeoff between prevention and detection of security attacks. Designing a voting system to prevent attack entirely may not be possible so an attractive alternative is to design mechanisms to detect attacks and recover from them.

- **Wholesale vs. Retail:** The researchers attempted to distinguish attacks that attempt to tamper with many votes (a “wholesale” attack) from attacks that attempt to tamper with only a few votes (a “retail” attack).
- **Casual vs. Sophisticated:** The researchers presumed that some attacks require little technical knowledge or sophistication, and, in contrast, other attacks require deep technical knowledge, specialized skill, or advance planning. The researchers studied both sophisticated attacks and casual, low-tech attacks.

Judgments about the probability of an attack or the impact on the election were specified in the report as outside the scope of the researchers’ review.

After creating the threat model, the Academic researchers reviewed Ohio’s election *procedures*. Election procedures are best practices, typically mandated by a county board of elections or the secretary of state to ensure that an election is carried out securely and correctly. Procedures are often as important as the technical security features of the election system. However, the researchers also presumed that given the human involvement in procedures, any procedure, no matter how well-crafted should be viewed as an “imperfect mitigation.” (*Id.* at 23.) Therefore, those setting procedures should carefully consider what happens when procedures are not followed.

## Findings

### Summary

The Academic researchers identified four “critical failures in design and implementation” of all three voting systems. (*Id.* at 3.)

- **Insufficient Security:** The voting systems uniformly “failed to adequately address important threats against election data and processes,” including a “failure to adequately defend an election from insiders, to prevent virally infected software . . . and to ensure cast votes are appropriately protected and accurately counted.” (*Id.*)
- **Security Technology:** The voting systems allow the “pervasive mis-application of security technology,” including failure to follow “standard and well-known practices for the use of cryptography, key and password management, and security hardware.” (*Id.*)
- **Auditing:** The voting systems exhibit “a visible lack of trustworthy auditing capability,” resulting in difficulty discovering when a security attack occurs or how to isolate or recover from an attack when detected. (*Id.*)
- **Software Maintenance:** The voting systems’ software maintenance practices are “deeply flawed,” leading to “fragile software in which exploitable crashes, lockups, and failures are common in normal use.” (*Id.*)

The Academic teams were able to provide a number of procedures that may mitigate or completely address identified security issues. However, in many cases, the teams could

not identify any practical procedures that will adequately address the security limitations. (*Id.*)

### **Specific Results: Source Code Analysis and Red Team (Penetration) Testing**

#### **ES&S**

The Academic researchers concluded that the central server and software and the precinct-based components, both DRE and optical scan voting machines (*i.e.*, the ES&S Unity Election Management System (EMS), iVotronic DRE and M100 optical scan systems) “lack the fundamental technical controls necessary to guarantee a trustworthy election under operational conditions.” (*Id.* at 29.) The researchers discovered “exploitable vulnerabilities” that allowed even persons with limited access – such as voters or poll workers – to compromise voting machines and election results, or to inject and spread software viruses into the central election management system. (*Id.*) Academic researchers concluded that these vulnerabilities arise from the following “pervasive, critical failures”:

- Failure to protect election data and software
- Failure to effectively control access to election operations
- Failure to correctly implement security mechanisms
- Failure to follow standard software and security engineering practices

(*Id.*)

Given that this was the first in-depth security analysis of the ES&S system, the Academic researchers concluded:

We believe the issues reported in this study represent practical threats to ES&S-based elections as they are conducted in Ohio. It may in some cases be possible to construct procedural safeguards that partially mitigate some of the individual vulnerabilities reported here. However, taken as a whole, the security failures in the ES&S system are of a magnitude and depth that, absent a substantial re-engineering of the software itself, renders procedural changes alone unlikely to meaningfully improve security.

(*Id.* at 30.)

Because the security failures of the ES&S system are “severe and pervasive,” the Academic research teams listed a voting system that uses only a centrally-counted optical scan hardware as an alternative system that may eliminate many of the precinct-based security attacks. (*Id.*)

#### **Failure to Protect Election Data and Software**

The researchers concluded that the firmware and configuration of the ES&S precinct hardware can be “easily tampered with” at the polling place. (*Id.* at 29.) Virtually every piece of precinct hardware could be compromised without knowledge of passwords and

without the use of any specialized proprietary hardware. (*Id.*) Some of the identified vulnerabilities included:

- Poll workers or voters can re-calibrate the screen of an iVotronic to prevent voting for certain candidates or to cause voter input for one candidate to be recorded for another. The procedure for re-calibrating required about one minute and is “largely indistinguishable from normal voter behavior.” (*Id.* at 50.)
- Access to certain PEBs could allow unauthorized individuals to alter poll-closing functions, such as the precinct’s reported vote tallies, and inject malicious code that could be transferred from memory cards to other DREs and memory cards to the board of elections’ central system or server. (*Id.* at 51.)
- The basic physical security features that protect precinct hardware – such as locks and seals – are “ineffective” or “easily defeated.” (*Id.* at 52.) For example, a primary mechanism for logging events on the iVotronic terminal is the RTAL printer. However, the cable connecting the printer is readily accessible to a voter and can be easily removed without tools or suspicious activity. (*Id.*)
- The Unity tallying system and the iVotronic terminal have “buffer overflow software bugs” that allow unauthorized individuals who can provide input on a removable storage media device, such as a PEB or memory card, to effectively take control over the system. A buffer overflow in input processing is a common type of programming error (that is, placing too much code in a memory-limited space) that has been responsible for many security failures in modern computing. (*Id.* at 53.) For example, the researchers experimentally proved that malicious code could be injected at the precinct level to change the votes of both inattentive voters and attentive voters monitoring the VVPAT. The researchers crafted a malicious PEB that overflowed the memory buffer and introduced it into the voting system. (*Id.* at 93-94.)
- Other identified vulnerabilities can be found in Chapters 7 and 9 of Appendix F.

### **Failure to Effectively Control Access to Election Operations**

The researchers concluded that access to administrative and voter functions are protected with “ineffective security mechanisms.” (*Id.* at 29.) Some of the identified vulnerabilities include:

- The iVotronic’s security mechanisms – such as passwords or firmware update functions – are “ineffective,” as the researchers found several practical ways to bypass each security mechanism and successfully replace or alter the iVotronic firmware, without knowledge of passwords or breaking any seals, such as when the polls are open. Any attack that compromises firmware is extremely serious, as the firmware controls every aspect of the ballot presented to the voters, the recorded votes, and the tally system. (*Id.* at 55.) For example, a firewall alteration was experimentally proved to fake a voter into believing that his or her vote was cast, although it was not. Seconds after the voter left the voting machine, the machine returned to the confirmation page, which resulted in a “fleeing voter” scenario, and the vote did not count. (*Id.* at 95-96.)



- The Unity software runs on an off-the-shelf operating system and therefore is “heavily dependent” on the local computing environment for its security. (*Id.* at 56.)
- Any person can load firmware into the M100 precinct optical scan with access to a PCMCIA card slot. Tamper seals may protect the slot, but researchers found that the seal may be bypassed. (*Id.* at 56.)
- The software or firmware of almost every major component can be altered or replaced by input from the other components with which it communicates. (*Id.* at 56.)

### **Failure to Correctly Implement Security Mechanisms**

The researchers concluded that many of the most serious vulnerabilities in the ES&S system arise from the incorrect use of security technologies such as cryptography. This effectively neutralizes several basic security features, exposing the system and its data to misuse or manipulation. (*Id.* at 29.) Some of the identified vulnerabilities include:

- The data on the M100 PCMCIA cards – the removable storage devices used to load ballot definitions and firmware into the M100 and to report vote tallies back to the Unity system at the board of elections office – are not cryptographically protected. Therefore, an unauthorized individual can “easily” forge or modify election results. (*Id.* at 57.)
- The iVotronic DRE uses cryptography to protect data on its removable storage devices – the PEB and the CF card. However, errors in its implementation render the protection “completely ineffective.” (*Id.*)

### **Failure to Follow Standard Software and Security Engineering Practices**

The researchers concluded that a root cause of the security and reliability issues present in the system is the “visible lack of sound software and security engineering practices.” (*Id.* at 29.) Examples include poor or unsafe coding practices, unclear or undefined security goals, technology misuse, and poor maintenance. This general lack of quality leads to a “buggy, unstable, and exploitable system.” (*Id.*)

### **Premier**

The Academic review concluded that the Premier system “lacks the technical protections necessary to guarantee a trustworthy election under operational conditions.” (*Id.* at 103.) Flaws in the system’s design, development, and processes lead a “broad spectrum of issues that undermine the voting system’s security and reliability.” (*Id.*) These vulnerabilities result in the following failures of Premier’s voting system:

- Failure to effectively protect vote integrity and privacy
- Failure to protect election from malicious insiders
- Failure to validate and protect software
- Failure to provide trustworthy auditing
- Failure to follow standard software and security engineering practices.

The researchers' findings were consistent with previous studies identifying vulnerabilities with the Premier system, which were conducted as early as 2001. After numerous reviews and new software and hardware upgrades, the researchers not only discovered the same problems as reported earlier but uncovered new serious issues as well. The researchers concluded: "[t]he review teams feel strongly that the continued issues of security and quality are the result of deep systemic flaws. Thus, we agree with previous analysis and observe that the safest avenue to trustworthy elections is to re-engineer the Premier system to be secure by design." (*Id.* at 104.)

### **Failure To Effectively Protect Vote Integrity and Privacy/Failure to Protect Elections From Malicious Insiders**

The researchers identified numerous vulnerabilities that could allow an unauthorized individual to "modify or replace ballot definitions, to change, miscount, or discard completed votes, or to corrupt the tally processes." (*Id.* at 103.) Furthermore, the Premier system does not provide adequate protections to prevent that election officials or vendor representatives do not manipulate the system or its data. (*Id.*) Some of the identified vulnerabilities include:

- The methods used to protect the integrity and privacy of important election data are circumventable. For example, the security protections on the memory cards – which are the central device for storing and communicating election data – are "ineffective" at preventing an unauthorized individual from viewing or modifying the data held on the card. (*Id.* at 114.) The memory cards for the precinct optical scan machine are completely "unprotected," and the memory cards for the DRE, the AV-TSX, while superficially protected by a "Data Key," are not "adequately protected." (*Id.*) The result is that an unauthorized individual who gains access to a memory card may modify elections results. The researchers experimentally proved that, because the memory cards for the DRE machines are encrypted using the same data key, a single compromised voting machine renders vulnerable the results on all other memory cards in the county. (*Id.* at 160.)
- The precinct-based optical scan and DRE machines "failed" to meet the goal of voter privacy, as the systems could be used in conjunction with poll books to determine voter choices. (*Id.* at 114.)
- The databases on the Premier GEMS server are "largely unprotected and can be freely accessed." (*Id.*) For example, access to GEMS functionality is governed by passwords that can be cracked using "standard password cracker tools." (*Id.*) Additionally, the audit logs, which provide an evidentiary trail of server usage, are not authenticated and are prone to forgery or alteration. (*Id.* at 162-63.)
- The use of many standard security technologies are "deeply flawed." (*Id.* at 113.) For example, the creation, storage, and use of the cryptographic keys used in the DRE and the GEMS server and connected EMP work stations to preserve the secrecy and integrity of election data are "insufficient to ensure an attacker cannot view or modify election data." (*Id.* at 115.) The Voter Card Encoders, used to allow voters to cast individual ballots, are not protected by a PIN or other security enhancement. Once a Voter Card Encoder is enabled, no additional security layer prevents unauthorized use to cast multiple ballots. (*Id.* at 171.)

- The Digital Guardian software, installed on the GEMS server to address already known security issues, is “circumventable” to render Digital Guardian inoperable and remove its protections. (*Id.* at 120.)
- Other identified vulnerabilities can be found in Chapters 13, 14, and 15 of Appendix F.

### **Failure to Validate and Protect Software / Failure to Follow Standard Software and Security Engineering Practices**

The researchers concluded that the Premier system makes only “limited and ineffective attempts to validate the software running within the system.” (*Id.* at 103.) As a result, an unauthorized individual may “exploit software and replace it with their own with little fear of detection.” (*Id.*) For example, because the components of the Premier system trust one another, a malicious GEMS server or DRE could crash an EMP. (*Id.* at 166.)

Additionally, errors in coding and design are concluded to be “widespread” in the Premier system. (*Id.* at 117.) These issues could lead to “serious vulnerabilities” that can affect the processes and accuracy of an election. (*Id.*) The researchers concluded that errors in the coding of the Premier system can be attributed to: complexity of the system components; lack of basic mechanisms to ensure integrity of the software; lack of security practices appropriate for its system; and over-reliance on commercial off-the-shelf software. (*Id.*)

### **Failure to Provide Trustworthy Auditing**

The researchers concluded that the auditing capabilities of the Premier system are “limited.” (*Id.* at 103.) The current auditing features are “vulnerable to a broad range of attacks that can corrupt or erase logs of election activities,” resulting in a severe limitation of election officials’ ability to detect and diagnose attacks. Moreover, because the auditing features are generally unreliable, recovery from attack may in practice be “enormously difficult or impossible.” (*Id.*)

### ***Hart***

The Academic researchers concluded that the Hart system “lacks the technical protections necessary to guarantee a trustworthy election under operational conditions.” (*Id.* at 197.) The vulnerabilities and features of the system work in concert to provide “numerous opportunities to manipulate election outcomes or cast doubt on legitimate election activities.” (*Id.*) These vulnerabilities result in the following failures of Hart’s voting system:

- Failure to effectively protect election data integrity
- Failure to eliminate or document unsafe functionality
- Failure to protect election from malicious insiders
- Failure to provide trustworthy auditing.

The researchers concluded that their findings are consistent with those of previous studies of the Hart voting system:

The lack of protections leaves the system vulnerable. Thus, the security of an election is almost entirely reliant on the physical practices. The technical limitations of its design further show that when those practices are not uniformly followed, it will be difficult to determine if attacks happened and what they were. Even when such attacks are identified, it is unlikely that the resulting damage can be contained and the public's confidence in the accuracy and fairness of the election restored.

(*Id.* at 198.)

### **Failure To Effectively Protect Election Data Integrity**

The researchers concluded that virtually every ballot, vote, election result, and audit log is “forgeable or otherwise manipulatable by an attacker with even brief access to the voting systems.” (*Id.* at 197.) The reason is that the mechanisms that Hart uses to protect data and software is frequently based on absent or flawed security models. The researchers concluded that “in most cases these issues cannot be addressed via software upgrades, but call for rethinking of both technical design and procedural practices.” (*Id.* at 208.) Some of the identified vulnerabilities include:

- Much of the data security in the Hart system flows from the single 32-byte key. The design of the Hart voting system therefore violates a basic isolation tenet of security engineering: compromise of a single precinct provides materials to compromise any precinct and election headquarters. If such compromise occurs, it will be impossible to identify which precinct is responsible for the attack. (*Id.* at 208.)
- Hart’s back-end or board office devices are networked to each other; however, Hart provides no device-to-device communication security, exposing critical data to an unauthorized individual who could generate voter codes, upload firmware, or erase voting or audit data. (*Id.* at 208-209.)
- The Hart software and firmware internal validity checks, where present, are “ineffective” at detecting compromises. (*Id.* at 209.) For example, in the case of the eScan (the precinct-based optical scanner), an unauthorized individual can replace the entire firmware with unobserved access to the eScan for 60 seconds, which would allow an unauthorized individual to completely alter election results on the Mobile Ballot Box (MBB) and the PCMCIA card. (*Id.*)
- Every authentication mechanism in the Hart system is “circumventable,” including the hardware tokens, passwords, PIN numbers, and voter codes. (*Id.*)
- Other identified vulnerabilities can be found in Chapters 19, 20, and 21 of Appendix F.

### **Failure To Eliminate Or Document Unsafe Functionality**

The researchers identified a number of largely undocumented features in the Hart system that are “highly dangerous” in an election system. (*Id.* at 197.) The Hart system consists of thousands of lines of code distributed over a large number of applications and developed over a decade by various developers. A byproduct of this process is a “large number of old, unused, and otherwise ‘orphaned’ features built into the software.” (*Id.* at 210.) The researchers concluded that these features present a source of security issues.

### **Failure To Protect Election From “Malicious Insiders”**

The researchers concluded that the protections in the Hart system that are intended to prevent election officials and vendor representatives from using dangerous features or modifying election data are “circumventable.” (*Id.* at 197.) Individuals with access to the voting system can quickly recover critical system passwords, extract cryptographic keys, and reproduce security hardware, which can ultimately “forge election data and compromise nearly all of the Hart election equipment.” (*Id.*)

### **Failure To Provide Trustworthy Auditing**

The researchers concluded the auditing capabilities of the Hart system are “limited.” (*Id.* at 197.) The auditing features provided are “vulnerable to a broad range of attacks that can corrupt or erase logs of election activities.” (*Id.*) This severely limits the ability of election officials to detect and diagnose attacks.

## **Summary of Boards of Elections Officials’ Review of the Academic Research Teams’ Findings on the Security Assessment of the State’s Voting Systems**

Two Democrats and one Republican boards of elections officials reviewed the Academic research teams’ findings on the security of Ohio’s three voting systems. Two of these officials utilize the Premier DRE voting system in their counties, while the third utilizes the ES&S DRE voting system in his or her county. In addition to the elections officials, the review group consisted of three secretary of state employees — a facilitator, an attorney, and a “scribe.” A “Capsule Summary Statement” of the elections officials’ review is provided below, basically as prepared by the “scribe,” along with a table summarizing this boards of elections review team’s standardized evaluation of the Academic teams’ findings.

### **Capsule Summary Statement by Boards of Elections (BOE) Team Reviewing the Academic Teams’ Findings**

#### **Part 1 of the Academic Report: Group Summary Statement**

Part 1 was well written and organized with a clear focus that generates an opinion. The report is created within a logical framework. At this introductory stage, the BOE officials posited that the report is generally based on pure supposition and bias. The BOE officials stated that the information in the Executive Summary, Overview and Threat Model was based on a variety of data intertwined with personal experience, finding that a large amount of information was unsubstantiated and biased and that the report

supported the biases of the authors in order to substantiate their claims. The BOE officials agreed that the claims are presented in a specific manner with a consistent point of view. Nonetheless, after reviewing Part 1, the BOE officials did not initially agree with the report or the conclusions contained within the report.

There was concern about the following statement contained in the report: “Doubt is often difficult to dispel. Lingering concerns often have a chilling effect on voters, and tend to color unrelated legitimate activities as well. Such concerns may continue for future elections.” (Academic Final Report at 16.) The BOE officials are concerned that the authors of the study could be placed in the position to be an “attacker” of voting systems. Therefore, they could have the ability to cast doubt on the election process, which would have a devastating effect on the election process. One BOE official expressed concern that the Academic reviewers appeared not to trust that election officials would make every effort to conduct a fair and honest election.

### **Part 2 of the Academic Report on ES&S: Group Summary Statement**

The BOE officials next reviewed the chapters of the Final Academic Report devoted to ES&S. The BOE officials agreed that this information was extensive and well developed but highly technical. The report contained numerous examples of security issues with the ES&S system and their impact on the system and the election process. However, the BOE officials believed they would have been able to gain a more accurate assessment if the report included a peer review. The BOE officials discovered some discrepancies in the use of footnotes. Additionally, the BOE officials’ most notable concern about the report was that solutions to these security issues were not presented.

The BOE officials described the language in the report as “over-hyped.” For example, the BOE officials highlighted the follow sentence: “additionally, the key blanks for a scanner and ballot box key are easily duplicated, so a compromise of either key could affect machines nation-wide.” (Academic Final Report at 73.) The BOE reviewers believed this language illustrated a biased view of the authors. The BOE officials concluded that a probability scale with a rating system of likely, unlikely and highly unlikely would have been a useful tool for those reviewing the report. Overall, the BOE officials agreed the report on ES&S rated between good and excellent, but the information was voluminous in nature and difficult for a layperson to comprehend. After a review of the ES&S section, the BOE officials did not agree with the information as presented in the report.

### **Part 3 of the Academic Report on Premier: Group Summary Statement**

The BOE officials next reviewed and evaluated the sections of the Academic Final Report devoted to the Premier voting system. The BOE officials concluded that these sections lacked sufficient evidence relating to real-life situations in which an attacker could circumvent the security of the voting system. Because the testing was completed in a controlled-academic setting, the BOE officials gave some areas of the report less weight and validity. The lack of performing these tests in real-life settings provided enough skepticism to cause the BOE officials to question the outcomes as fact-based realities. There was also a concern that the review team had a slightly higher bias toward Premier than other systems. The BOE officials were unclear whether the prior reports on Premier could be attributed to be the cause of this bias, or whether the review team simply replicated experiments within the prior study with a few minor adjustments. For example, the Academic researchers tested voter privacy by stacking ten ballots in the ballot box. The BOE officials agreed that a proper sample for real-life application would

be a test of 350 ballots.

The BOE officials believed the report had a clear and consistent point of view. However, there were several inconsistencies within the report, as well as mechanical errors. For example, there were incorrect statements about the supervisor smart card. The BOE officials agreed that the terminology created a mistrust of election officials by using the term "malicious election officials." The BOE officials felt this reference "planted seeds" in the mind of the public to mistrust those who oversee elections. The report also minimizes mitigation, allowing the problems with the voting systems to seem larger and more complex. The lack of procedural mitigations offered was a disappointment for the group. The BOE officials found the report gave more credibility to the problems than the solution. Generally speaking, the BOE officials found that the report supports a certain political spectrum that believes that all electronic voting equipment is unsafe and evil.

The amount of mechanical errors contained within the report caused the BOE officials to question the validity of certain assertions, but it was not sufficient to compromise the credibility of the report. The study is based on clinical testing with a limited view.

#### **Part 4 of the Academic Report on Hart: Group Summary Statement**

The BOE officials next reviewed and evaluated the sections of the Academic Final Report devoted to the Hart voting system. The BOE officials concluded that the report was written in a coherent fashion with scenarios that could be understood. The report presented various problems that could affect any election with any voting system. The problems stated throughout the report were not unique to the Hart system. The BOE officials believe there were several test assessments that could have been performed with punch cards and lever machines. There were some claims that BOE officials believed to be outside the scope of real-world applications, and there were instances where the BOE officials found that the data contradicted the researchers' claims. The BOE officials suggested that some logical conclusions were not presented as solutions. The flaws in logic found by these BOE officials led them to conclude that these flaws created a lingering doubt over the previously reviewed sections of the report relating to ES&S and Premier.

However, the sections devoted to the Hart voting system suggested more evidence of mitigation. In general, the BOE officials found this section of the report did offer solutions that were feasible and reasonable. The BOE officials believed that the review team could confirm their findings, because the source code was detectable. It was the general consensus that the material presented could have harsh ramifications in an elections context. The group suggested that many of the problems in the report could also happen with a simple desktop computer system. Further, the BOE officials found that some of the conclusions required leaps in logic that could not be related to real-world situations. There were questions of practicality and poor reasoning within the report. Specifically, the BOE officials found that the report itself could be viewed as an attack on the election system. The BOE officials found that the context of the situations needs further clarification in order to be clearly stated and supported.

**Summary Table of Standardized Evaluations by Boards of Elections Team  
Reviewing the Academic Teams' Findings**

**Average Academic Security Report Quality Ratings by Election Officials**

Quality	Scale	Executive Summary	ES&S	Hart	Premier
Data	1-3	2.3	3.0	2.7	2.7
Claims	1-3	3.0	3.0	3.0	2.7
Warrants	1-4	2.5	3.0	2.7	3.0
Coherence	1-4	3.7	4.0	4.0	3.3
Overall	1-5	4.3	4.7	4.3	4.3

Note. This table represents the average ratings of three election officials.

**Report Quality Rating Scales**

Scale	Dimension Measured
Data	Conclusions were based on and supported by data.
Claims	Claims were clear, consistent, feasible, and related to solutions
Warrants	Arguments were reliable, trustworthy, and logical
Coherence	Material was integrated and contained sufficient context
Overall	Overall report quality from failing to excellent



## **Configuration Management Assessment**

### **SysTEST**

The SysTest Risk Assessment Team performed a configuration management assessment of Premier, ES&S, and Hart InterCivic voting systems. The purpose of SysTest's assessment was to evaluate the secretary of state's ability to independently verify that the configuration of each voting system as approved for use by respective jurisdictions was consistent with, and unchanged from, the configuration certified by the State of Ohio, and that the certified configuration remained unchanged during all parts of the election process, including tabulation, during which results potentially could be affected. As part of its assessment, SysTest examined the processes and procedures used by the State of Ohio to manage the equipment configuration in the field, with particular interest given to how upgrades are managed and controlled. SysTest also examined whether the logic and accuracy (L&A) procedures in use by counties include steps for the verification of the hardware, firmware, and software versions in use.

SysTest created two reports: (1) an Executive Summary report and (2) a Final Technical Report. This Secretary's Report briefly explains SysTest's methods and findings. The complete SysTest reports are attached at Appendix G.

### **Method**

- **Physical Configuration Audit:** Initially, SysTest verified and recorded the revision levels (essentially the extent to which something is revised through updates, upgrades, etc.) of the hardware, firmware, and software of each voting system. SysTest then compared this information against documented revision levels of state-certified voting systems to verify if the systems in use by the sample of counties were versions certified by the State of Ohio.
- **Processes and Procedures:** SysTest assessed the processes and procedures used by the State of Ohio to manage the configuration of equipment in the field. This assessment was intended to determine if the successful operation of the equipment in an election is at risk due to incompatible hardware or inadequate processes designed to control and manage the configuration of the equipment.
- **Logic and Accuracy:** Additionally, SysTest conducted a review of L&A testing procedures used by a set of 11 counties specifically chosen by the secretary of state to ensure diverse representation. The purpose was to examine the level of consistency across Ohio's certified and deployed voting equipment, and whether the L&A procedures in place included appropriate steps for the verification of hardware, firmware, and software.

## **Findings**

### **Summary**

The physical configuration audit and assessment of configuration management procedures identified risks to be addressed. Summaries of the risks from a configuration management perspective are as follows:

1. The use of materials (specific memory storage devices, printer paper, etc.) that have not been certified by the manufacturers, but that are readily available on the open market, could “create significant risks.” (Final Technical Report at 58.)
2. To verify that the firmware/software installed on voting machines in use in the various counties is actually the certified version, any such possible procedure used before or after an election would be “impractical for current ES&S and Premier systems.” These systems require “disassembly of the unit, physical extraction of the memory device, and utilization of specialized equipment to read the data.” (*Id.* at 58, 59.)
3. Dissemination of technical specifications, standards and information to the counties, including those for L&A testing procedures to ensure a voting machine will accurately count votes, is not standardized, and therefore, L&A procedures throughout the state are inconsistent. (*Id.* at 59.)
4. Revisions to voting system software of all systems from county-to-county are unknown and not documented or tracked. (*Id.* at 59.)

### **Configuration Management Assessment: Specific Results and Suggested Improvements**

#### **Hart InterCivic**

SysTest concluded that “the installed and as-built configuration (defined by hardware, firmware, and software revision levels) of the Hart InterCivic voting system equipment in Ohio counties is unknown.” (*Id.* at 59.) To address this, SysTest suggests providing “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.” (*Id.*)

Further, SysTest determined that the Hart InterCivic SERVO software system provided to SysTest for analysis “was missing a file necessary for verifying the hash codes of the operating software,” thus indicating that the software installed in the counties’ voting system equipment “may not be equivalent to the certified version.” (*Id.* at 60.) As a possible mitigating factor, SysTest suggests that the secretary of state’s office “produce and distribute media containing a complete binary image of the certified version of

software to be installed on a voting machine,” and subsequently use the Hart InterCivic utility to verify that the loaded software is authentic, reloading the image from the supplied media should the software be found not to be the equivalent of the certified version. (*Id.* at 60.)

Additionally, SysTest determined “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.” (*Id.* at 60.) SysTest recommends verifying that the procedure provided by Hart is “disseminated to all counties that have Hart InterCivic equipment,” and that BOE personnel are properly educated on the use of the procedure. SysTest also recommends this procedure should be utilized every time the equipment is prepared for use, documenting the results of the verification. (*Id.* at 60.)

SysTest concluded that L&A procedures are not consistent throughout the counties using the Hart InterCivic voting system or have not been provided to the county boards of elections by the secretary of state’s office by directive. (*Id.* at 59.) SysTest recommends the secretary of state “provide a centralized source” for disseminating such information. (*Id.* at 59.)

Finally, Hart InterCivic has certified specific consumables and storage devices for use with its voting system, but uncertified forms of these materials are readily available on the open market. SysTest concluded that the use of uncertified consumables and storage devices present the most severe risk, in terms of configuration management, to the Hart InterCivic voting system, and could result in “significant failures during an election.” (*Id.* at 59.) This risk appears magnified by the fact that safeguards cannot be built into the system to ensure storage cards, thermal printer paper, ballot paper, and ballot fonts are the types certified for use. (*Id.* at 59.) SysTest recommends that the secretary of state “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,” and “clearly communicate to the BOE personnel that using something other than the specified materials may result in failures during an election.” (*Id.* at 59.)

### **ES&S**

Because SysTest “encountered an ES&S iVotronic unit that had down level software installed,” SysTest concluded that “the installed and as-built configuration (defined by hardware, firmware, and software revision levels) of the ES&S voting system equipment in Ohio counties is unknown.” (*Id.* at 61.) To address this, SysTest suggests providing “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.” (*Id.* at 61.)

Further, SysTest determined that the ES&S election management software system provided to SysTest for analysis “was missing files,” thus indicating that the software

installed in other voting system equipment in the counties “may not be equivalent to the certified version.” (*Id.* at 61, 62.) As a possible mitigating factor, SysTest suggests that the secretary of state’s office “produce and distribute media containing a complete binary image of the certified version of software to be installed on a voting machine,” verify that the loaded software is authentic, and reload the image from the supplied media should the software be found not to be the equivalent of the certified version. (*Id.*)

Additionally, SysTest analyzed the ES&S system for the purpose of recommending 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. SysTest concluded that “the procedure would be impractical to perform on all units in the field,” because it “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.” (*Id.* at 62.) SysTest further states that this process is “possible” but “cumbersome,” and “can only be performed by qualified personnel.” (*Id.*) SysTest further asserted that not practically being able to perform such a procedure on each machine presents severe risks to election integrity, as the firmware in the iVotronic voting machine could be “compromised and modified without detection,” conceivably occurring “before, during or after an election.” (*Id.*) SysTest suggests that the State of Ohio, as a mitigating factor, “require all manufacturers to implement an automated software routine,” for comparing the configuration of each machine in use with the certified configuration, and further suggests that the secretary of state should include such a process in state certification requirements. (*Id.*)

SysTest concluded that L&A procedures are not consistent throughout the counties using the ES&S voting system or have not been provided to the county boards of elections by the secretary of state’s office by directive. (*Id.* at 61.) SysTest recommends the secretary of state “provide a centralized source” for disseminating such information. (*Id.*)

Finally, ES&S has certified specific consumables and storage devices for use with its voting system, but uncertified forms of these materials are readily available on the open market. SysTest concluded that the use of uncertified consumables and storage devices present a severe risk to the ES&S voting system, and could result in “significant failures during an election.” (*Id.*) This risk appears magnified by the fact that safeguards cannot be built into the system to ensure storage cards, thermal printer paper, ballot paper, and ballot fonts are the types certified for use. (*Id.*) SysTest recommends that the secretary of state “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,” and “clearly communicate to the BOE personnel that using something other than the specified materials may result in failures during an election.” (*Id.*)

### **Premier**

SysTest concluded that “the installed and as-built configuration (defined by hardware, firmware, and software revision levels) of the Premier voting system equipment in Ohio counties is unknown.” (*Id.* at 62, 63.) To address this, SysTest suggests providing “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.” (*Id.*)

Additionally, SysTest analyzed the Premier system for the purpose of recommending 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. SysTest concluded that “the procedure would be impractical to perform on all units in the field,” because it “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.” (*Id.* at 63.) SysTest further states that this process is “possible” but “cumbersome,” and “can only be performed by qualified personnel.” (*Id.*) SysTest suggests that the State of Ohio, as a mitigating factor, “require all manufacturers to implement an automated software routine,” for comparing the configuration of each machine in use with the certified configuration, and further suggests that the secretary of state should include such a process in state certification requirements. (*Id.*)

SysTest concluded that L&A procedures are not consistent throughout the counties using the Premier voting system or have not been provided to the county boards of elections by the secretary of state’s office by directive. (*Id.* at 61.) SysTest recommends the secretary of state “provide a centralized source” for disseminating such information. (*Id.* at 63.)

Finally, Premier has certified specific thermal printer paper and certain storage devices for use with its voting system. SysTest concluded that the use of materials other than those specified could result in “significant problems.” (*Id.* at 58.) This risk appears magnified by the fact that safeguards cannot be built into the system to ensure only certified consumables and storage cards are used in a Premier voting system. (*Id.* at 63.) SysTest recommends that the secretary of state “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,” and “clearly communicate to the BOE personnel that using something other than the specified materials may result in failures during an election.” (*Id.*)

### **Summary of Board of Elections Officials’ Review of SysTest’s Findings on Configuration Management of the State’s Voting Systems**

One Republican and one Democrat boards of elections official each reviewed SysTest’s findings on the configuration management of Ohio’s three voting systems. Both of these officials utilize the ES&S Optical Scan voting system in their respective counties. In addition to the elections officials, the review group consisted of three secretary of state employees — a facilitator, an attorney, and a “scribe.” A “Capsule Summary Statement” of the elections officials’ review is provided below, basically as prepared by the “scribe,” along with a table summarizing this boards of elections review team’s standardized evaluation of SysTest’s findings.

**Capsule Summary Statement by Boards of Elections Team Reviewing  
SysTest's Findings on Configuration Management**

Although the purpose of the project and testing undertaken were clear and the findings credible, board of elections reviewers had to make assumptions as to how the testers arrived at their conclusions. Board officials found that the contractor did a good job of identifying the inadequacies of vendor products; however, there was not enough detail in the method, logic, or failure modes reported in the test results.

The board officials found that SysTest's recommendations to advertise the need for vendor-required supplies and the need for a common reference database of certified software and hardware versions of county equipment are good ones. However, this report needs to be revised to address:

- Inaccuracies in detail of some findings related to the use of the required thermal paper, ballot stock and fonts;
- The readability and annotations of tabular findings, the addition of footnotes, and consistent labels; and
- An important clarification regarding the specifics of the 2006 secretary of state directive regarding logic and accuracy testing; specifically, the availability of a procedure for logic and accuracy testing. [No such directive has been located in the secretary of state's office since the new administration took over in 2007.]

**Summary Table of Standardized Evaluations by Board of Elections Team  
Reviewing SysTest's Findings on Configuration Management**

**Average Configuration Management Report Quality Ratings by Election Officials**

Quality	Scale	Executive Summary	ES&S	Hart	Premier
Data	1-3	2.0	2.0	2.0	2.0
Claims	1-3	2.0	2.0	2.0	2.0
Warrants	1-4	2.0	2.0	2.0	2.0
Coherence	1-4	2.5	2.5	2.5	2.5
Overall	1-5	3.0	3.5	3.5	3.5

Note. This table represents the average ratings of two election officials.

**Report Quality Rating Scales**

Scale	Dimension Measured
Data	Conclusions were based on and supported by data.
Claims	Claims were clear, consistent, feasible, and related to solutions
Warrants	Arguments were reliable, trustworthy, and logical
Coherence	Material was integrated and contained sufficient context
Overall	Overall report quality from failing to excellent

## Performance Testing

### SysTEST

SysTest executed “performance testing” to assess if there were risks to the integrity of the election and accuracy of the vote counts during simple use of each of the certified voting systems. SysTest created test cases to observe the result of any possible deficiencies in an election process. SysTest’s performance testing emphasized preparing for an election, the accuracy and integrity of the voting process, and the accuracy of audit logs.

SysTest created two reports: (1) an Executive Summary report and (2) a Final Technical Report. This Secretary’s Report briefly explains SysTest’s methods and findings. The complete SysTest reports are attached at Appendix G.

### Method

SysTest developed a performance test plan and associated test cases that defined its approach in executing performance testing on the ES&S Unity server software, Premier GEMS server software, and Hart InterCivic Ballot Origination, Tally, Rally, and SERVO election management software components. The purpose of this 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 needed 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 is a summary of each test case:

- **Election Creation** – The object of this test case is to observe the difficulty or ease of creating an election.
- **Set-up and Closure of Polling Place** – The object of this test case is to observe the difficulty or ease of setting up the election system at board of elections office and polling locations, loading the election, and opening and closing the polls.
- **Configuration Management** – The object of this test case is to verify the versions of software and hardware used in the election system.
- **DRE Functionality** – The object of this test case is to verify the functionality of the DRE in performing administrative duties.
- **Election Vote Consolidation (Primary and General)** – The object of this test case is to verify that the vote totals obtained from each type of supported

voting device (optical scan or DRE) can be accurately consolidated into a central count vote total and that all required reports and audit records can be viewed and/or produced.

- **Voter Verified Paper Audit Trail (VVPAT) Accuracy** – The object of this test case is to test and verify both the functionality and accuracy of a VVPAT printer device associated with a DRE polling location, confirming whether all votes are accurately captured on the paper trail, that they are readable, that they can be cancelled and changed by the voter, and that the VVPAT accurately reflects the correct changes.
- **Load Test Early Voting** – The object of this test case is to verify that votes are not lost due to memory leak while casting ballots on a DRE in Early Voting Mode when its memory capacity is exceeded, to verify that in such cases a warning message is given to a user, and to verify the accuracy and integrity of the tally.
- **Load Test DRE** – The object of this test case is to verify that votes are not lost due to insufficient memory capacity while casting ballots on a DRE in Election Day Mode.
- **Load Test Optical Scan** – The object of this test case is to verify that votes are not lost due to insufficient memory capacity while casting ballots on an Optical Scan device in Election Day Mode.
- **Load Test Storage Components** – The object of this test case is to verify a warning message is given to the user when the user attempts to load an election definition that exceeds the memory capacity of the external memory device.
- **Security** – The object 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.
- **PCMCIA Card Batch Testing** – The object of this test case is to verify all PCMCIA cards (memory cards or devices) provided for testing will function according to system specifications.
- **Audit Tape** – The object of this test case is to verify the election system will log all activities on each component (server, DRE, scanner, etc.) of the system.

(Final Technical Report, at 14, 15.)

## Findings

### Summary

SysTest’s risk assessment process “uses a combination of the probability of occurrence and the impact of the occurrence, should it occur.” (Final Technical Report at 16.) SysTest’s performance testing of the Premier, ES&S, and Hart InterCivic voting systems identified numerous risks to election integrity, ranging from minor to severe. Most significantly, SysTest found one severe risk with each the Premier and ES&S system.



(Executive Summary Final Report at 16.) This report focuses on summarizing the moderate and severe risks identified by SysTest for all systems, categorized in their table of results as “yellow” and “red.” (Final Technical Report at 68-73)

**Performance Assessment:**  
**Specific Results and Suggested Improvements**

**Premier**

SysTest identified several moderate risks, and one severe risk to election integrity when testing the Premier GEMS voting system, TSX DRE voting machines (used at the precinct level), and the AccuVote optical scanners (used at both the precinct level and at the board of elections for central count), as summarized below.

Several of the moderate risks identified were in relation to proper documentation provided to boards of elections staff for installing the voting system. Specifically, SysTest found that Premier’s user manuals or guides lacked sufficient information for configuring the AccuVote central count operating system, which could result in delays or improper set-up of equipment. (*Id.* at 65, 66, 68, 69.)

SysTest also identified documentation issues relating to the use of the VVPAT for the TSX DRE printer. VVPAT thermal paper can easily be installed backwards, which would cause no votes to be recorded on the thermal paper used for the VVPAT. Premier’s documentation does not address these issues, and its Poll Workers Guide states that in the event that a VVPAT does not write, it should be taken out of service, which may be a needless measure (and decrease the number of available machines in times of heavy voter turnout). (*Id.* at 65, 66, 69, 70.) SysTest additionally indicated that the TSX did not initially recognize the memory card that contained the election to be loaded unless the memory card was removed and reinserted. This could potentially lead a poll worker to believe the memory card is defective. (*Id.* at 71.)

As a mitigating factor relating to the above documentation issues, SysTest recommends supplemental documentation and/or training be provided to election administrators. (*Id.* at 69, 71.)

Additionally, SysTest identified that Premier’s GEMS Server Configuration Guide may mislead an election administrator to disable a particular service, which in turn, could result in insufficient performance or procedural delays on Election Day. (*Id.* at 66, 69.) To mitigate these risks, SysTest recommends that the server administrator perform a full configuration check before the election. (*Id.* at 69.)

When SysTest performed further testing on the Premier TSX DRE, the VVPAT did not list the entire final ballot for the voter’s verification, which could lead to “voter discontent.” (*Id.* at 70.) Additionally, if a candidate has an unusually long name, the VVPAT will cut off the name at 20 characters, potentially leading to voter confusion. (*Id.* at 66, 67, 70.) SysTest suggests conducting logic and accuracy (L&A) testing on the

VVPAT prior to opening the polls, and if problems occur, recalibrating the VVPAT. (*Id.* at 70.)

SysTest identified that changing the ballot style of paper ballots in the Premier GEMS system at the “last minute,” caused “AccuVote OS [optical scan] (1.96.6) to ignore one race.” (*Id.* at 71.) SysTest suggests “a complete L&A needs to be conducted on absentee ballots with every single race being voted.” (*Id.* at 71.)

Finally, the most severe risk identified in performance testing of the Premier voting system was during a load test on the TSX DRE. SysTest discovered that the TSX DRE erases vote data on the memory card during the voting process when memory capacity is exceeded on the memory card. (*Id.* at 69.) If failure occurs, the official ballot count would have to be conducted by hand using the VVPAT records, which would be tedious and laborious. (*Id.* at 69.) To mitigate this risk, SysTest suggests limiting the number of voters that can vote on a TSX, which can be calculated by establishing the amount of free space that exists on the card and how much space is consumed by each ballot cast.

### **ES&S**

SysTest identified numerous moderate risks and two severe risks to election integrity when testing the ES&S Unity voting system, which includes the iVotronic DRE (used at the precinct level), M100 optical scanner (used at the precinct level), and M650 optical scanner (used at the board of elections for central count). The various risks are summarized below.

SysTest identified that the Unity voting system does not mandate the need to change usernames and passwords (used to access voting equipment during an election) from the default passwords supplied from ES&S documentation. The iVotronic machines tested were accessed by default common and identical usernames and passwords. (*Id.* at 82, 84, 89.) SysTest indicates that this could result in unauthorized personnel changing settings on voting equipment and suggests that the state “mandate that all passwords be changed and only revealed to necessary personnel,” and that “election officials should change the passwords occasionally for security purposes.” (*Id.* at 82, 84, 89.)

SysTest identified that the physical stability of the iVotronic DRE is “fragile,” and the use of these machines over several election cycles makes them susceptible to tipping over and becoming damaged. If damage to a machine occurred on Election Day, a polling location could experience a shortage of DREs. (*Id.* at 88, 89.)

The iVotronic DRE exists in 12-inch and 15-inch versions. SysTest identified that on the 12-inch iVotronic DRE, write-in instructions are not fully displayed on the write-in screen, which could create an obstacle in casting a write-in vote and cause “voter discontent.” (*Id.* at 84, 89.)

SysTest identified that the power supply of iVotronic’s Real Time Audit Log (RTAL), which is ES&S’s version of a VVPAT, is concealed and not readily apparent to poll workers. (*Id.* at 89.) SysTest discovered that if the power supply is not switched to “on”

before the iVotronic screen is locked into position, the RTAL does not work, even though the iVotronic machine itself will operate on battery power and display a message describing the “lack of its RTAL printer.” (*Id.* at 83.) These issues could lead to a poll worker believing that the entire unit is defective, taking it out of service and thereby a shortage of available machines. (*Id.* at 89.) As a mitigating factor to the above risks, SysTest suggests that poll workers fully inspect each DRE as part of their pre-election procedures. (*Id.* at 89.)

Additionally, SysTest identified connectivity issues with the iVotronic RTAL printer, which is located inside the voting machine but connected externally, and the Seiko report printer, which is a separate unit that must be connected via the same external serial port as the RTAL printer. SysTest states, “the connector between the iVotronic and the RTAL printer does not screw into place and may be removed by any voter and left in a position that its removal may not be obvious.” (*Id.* at 83.) If such a disconnection occurs, the iVotronic will not accept any additional votes until the RTAL printer connector is properly reattached. (*Id.* at 83.) If a poll worker wishes to print specific reports, he or she must disconnect the RTAL printer, and connect the separate Seiko report printer. If the poll worker attempts to print specific reports on the iVotronic but fails to physically change the printer, the reports will be temporarily lost. (*Id.* at 89.) Additionally, the iVotronic does not detect when the report printer is disconnected or turned off during printing, so the user must be aware of what he or she expects to be printed and be “cognizant of the printer’s status.” (*Id.* at 84.)

SysTest also states that a routine change from the RTAL printer to the report printer may result in a bent serial connector pin. In the case of a damaged pin, the serial cable and subsequently the RTAL and voting machine may become unusable. SysTest suggests updating training materials to emphasize the risks associated with changing the printer and keeping extra serial cables on hand to mitigate these risks. (*Id.* at 83, 89.)

SysTest identified moderate risks associated with the AutoMARK Voter Assist Terminal (VAT), an ADA-compliant ballot marking and reading device<sup>1</sup> not manufactured by ES&S, but made compatible with the ES&S Unity voting system. Specifically, SysTest found that the AutoMARK does not always recognize the inserted ballot, and when this occurs, the user must eject and reinsert the ballot as many as three times. (*Id.* at 82, 83, 90.) SysTest states, “This will cause voter discontent, confusion, and loss of confidence.” (*Id.* at 90.) SysTest suggests supplemental instructions be provided at the polling location, and increased awareness to this issue in poll worker education. (*Id.* at 90.)

Additionally, SysTest identified the character sets available for use for write-in votes on the AutoMARK differ from those available on the iVotronic DRE, specifically that the iVotronic DRE’s write-in display includes comma (,) and period (.) characters. SysTest states, “The difference in the available character sets may result in vote consolidation errors,” (*Id.* at 83.) and “This will delay reporting results.” (*Id.* at 90.)

SysTest further discovered that when the brail caption button was used, the AutoMARK’s display scrolling sometimes becomes “erratic,” which at times makes it “impossible to completely see the contents of a race’s display box.” (*Id.* at 82, 90.) SysTest states this

---

<sup>1</sup> This device reads a barcode on a pre-printed optical scan ballot that is inserted into the device, which is designed to recognize the ballot style. The device allows the voter to utilize its touch screen to mark the ballot but not tabulate it. Once marked, the ballot is ejected by the device to be read by an optical scanner. This device is frequently used by voters with disabilities.

will result in a “loss of voter confidence” and voter “confusion” and “discontent.” (*Id.* at 90.) As a mitigating factor, SysTest suggests supplemental instructions be provided at polling locations and increasing voter education. (*Id.* at 90.)

SysTest’s performance testing on the ES&S M100 and M650 optical scanners (used at both the precinct level and at boards of elections for central count) identified the following concerns. The M100 optical scanner has an attached metal ballot box, which should contain a diverter for the purpose of separating write-in ballots from normal ballots. Of the three M100 ballot boxes tested, only one contained the required write-in diverter. Without such a diverter, finding and tallying write-in votes “could be a difficult task,” and could result in a “delay tallying the write-ins.” (*Id.* at 87, 89.) SysTest suggests boards of elections conduct a full inspection as part of their pre-election process. (*Id.* at 89.)

SysTest identified that the M100 (precinct-based optical scanner) “does not scan incomplete marks reliably or consistently.” (*Id.* at 86.) SysTest found that incomplete marks are inconsistently recognized – sometimes recognized as votes, sometimes generating an “unreadable marks” message, and sometimes described as undervotes. SysTest states, “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.” (*Id.* at 86.) SysTest suggests several mitigating factors in relation to the M100’s inconsistency relating to incomplete marks, including first ensuring that the M100 is properly configured to reject “unreadable marks,” so the voter receives warnings that his or her marks are unreadable by the scanner. Additionally, SysTest suggests that it is important to educate voters on how to properly fill in ballot ovals, and also suggests that instructions be posted at polling sites for voters to completely darken intended ballot ovals. (*Id.* at 86, 87, 89.)

Additionally, SysTest identified that while printing reports, the M100 does not detect when printer paper runs out, rather it continues printing to nothing and the “print output is lost.” (*Id.* at 86, 90.) SysTest recommends that poll worker training be updated to note this, to verify there is adequate paper prior to printing, and for poll workers to increase their awareness of what is being printed to determine whether something is lost due to insufficient paper. (*Id.* at 86, 90.)

In testing the M650 (high-speed optical scanner), SysTest discovered that the scanner only reads ballot ovals in the either right or left column, depending on how the election administrator configures the ballot definition of the machine. SysTest states, “There is a risk that ballots with ovals on the wrong side could be printed and therefore be unreadable by an M650.” (*Id.* at 85, 90.) Therefore, it is imperative that boards of elections employees create ballots in the correct template, or else votes may not be read correctly. (*Id.* at 85, 90.)

The most severe risk SysTest identified with the M650 is that in order for vote data to be written to its internal hard drive, the user is required to manually save it from the internal RAM to the hard drive. If a power failure occurs, the scanned ballots in the RAM are lost and it becomes necessary to re-scan all ballots processed since the last prior save. “If such ballots are not reprocessed, then those votes will not be counted.” (*Id.* at 88.) SysTest concludes, “It is critical that batches be processed in their entirety,

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.” (*Id.* at 85, 90.)

SysTest also identified a severe risk inherent in both the M100 and M650 optical scanners. The M100 and M650 scanners do not mark ballots as having been processed. Because of this, “paper ballots can be scanned more than once,” and “a person with malicious intent can skew the election results.” (*Id.* at 89, 90.) SysTest suggests that all batches should be processed in their entirety, and the handling procedures in place must include a political balance of staff handling them. (*Id.* at 89.)

Additionally, SysTest identified a risk inherent to the Election Reporting Manager application, specifically regarding the handling and importing of vote results from the M100 and M650 memory devices to the reporting application. SysTest states, “There are no safeguards inherent in the system to prevent a user from importing vote results from the same memory devices multiple times. System operators should store processed memory devices in a secure location physically segregated from unprocessed media devices immediately after processing them.” (*Id.* at 88.)

### **Hart InterCivic**

SysTest identified two moderate risks to election integrity when testing the Hart InterCivic voting system, which includes the Ballot Origination, Tally, Rally, and SERVO election management software components, the eSlate DRE, and the eScan optical scanner (used at the precinct level).

Initially, SysTest identified through their performance testing that the Hart InterCivic system is “not as feature rich a voting solution as the ES&S and Premier,” and does not offer “the flexibility in election definition and ballot design capabilities.” (*Id.* at 91.) Because of this, the Hart system is “far less complex,” and has “fewer potentials for risks.” (*Id.* at 91.) The two moderate risks identified by SysTest are summarized below.

Both moderate risks with the Hart InterCivic system, as identified by SysTest, involve a console called the Judge’s Booth Controller (JBC). The JBC is a single console that attaches to and can control as many as 12 eSlate DREs for the purpose of generating voter access codes and delivering ballot configurations to the DREs, recording records of votes cast, storing ballots to its internal memory, and is capable of accumulating and reporting vote results.

SysTest identified that “one JBC cannot be used for early voting and Election Day processing,” which would force small counties to purchase two units. (*Id.* at 93.) Additionally, when an audit log was created, the log failed to record when the JBC was powered down and powered up. Because of this, an audit log would not be able to determine how long a JBC unit was powered down. “This could hamper any inquiries if a re-creation of Election Day events needs to be created.” (*Id.* at 93, 94.) As a mitigating factor, SysTest suggests requiring constant monitoring of JBC units. (*Id.* at 94.)

## **Summary of Board of Elections Officials' Review of SysTest's Findings on Performance Testing of the State's Voting Systems**

One Republican and one Democrat boards of elections officials reviewed SysTest's findings on the performance testing of Ohio's three voting systems. One of these officials utilizes the Premier DRE voting system and the other utilizes the ES&S optical scan voting system in their respective counties. In addition to the elections officials, the review group consisted of three secretary of state employees — a facilitator, an attorney, and a "scribe." A "Capsule Summary Statement" of the elections officials' review is provided below, basically as prepared by the "scribe," along with a table summarizing this boards of elections review team's standardized evaluation of SysTest's findings.

### **Capsule Summary Statement by Boards of Elections Team Reviewing SysTest's Findings on Performance Testing**

Board of elections officials found the SysTest performance testing report to be complete and thorough. The problems SysTest identified did not come as a surprise to any of the election officials, as the election officials have already encountered such problems. The suggestions offered by SysTest for risk mitigation were found to be realistic and sufficient; however, the officials believed that boards of elections have already taken many of the suggested steps.

The election officials believe that the biggest threat to elections is the complexity of the voting systems in concert with human error, and SysTest's report successfully reflects that. The election officials did not identify glaring deficiencies regarding the subjects the report covered and solutions the report offered.

Overall, the election officials felt the SysTest report was very good, identifying as the report's only shortfall the lack of information and data on the Hart InterCivic system. The election officials agreed that the report could not be accused of being inflammatory or alarmist, especially because mitigating factors were offered for the equipment performance risks SysTest identified.

The election officials believe voting machine manufacturers can take the information in this report and use it as a good working tool to fix some of the faulty elements present in voting systems. The election officials also believe the secretary of state can issue advisories and directives to help alleviate some of the issues documented in this report.

The main point the election officials took from this report is that the systems *perform*, but they can perform more *efficiently* and *securely* if some of the suggestions offered in the report are implemented.

**Summary Table of Standardized Evaluations by Board of Elections Team  
Reviewing SysTest's Findings on Performance Testing**

**Average Performance Report Quality Ratings by Election Officials**

Quality	Scale	ES&S	Hart	Premier
Data	1-3	3.0	2.0	3.0
Claims	1-3	3.0	1.5	2.0
Warrants	1-4	4.0	2.5	4.0
Coherence	1-4	4.0	3.0	4.0
Overall	1-5	4.0	3.0	4.5

Note. This table represents the average ratings of two election officials

**Report Quality Rating Scales**

Scale	Dimension Measured
Data	Conclusions were based on and supported by data.
Claims	Claims were clear, consistent, feasible, and related to solutions
Warrants	Arguments were reliable, trustworthy, and logical
Coherence	Material was integrated and contained sufficient context
Overall	Overall report quality from failing to excellent

## **Elections Operations and Internal Control Assessment**

### **SysTest**

The SysTest Risk Assessment Team performed an elections operations and internal control assessment of existing or proposed policies, procedures, and internal controls established in manufacturer documentation and county boards of elections (“BOE”). The purpose of SysTest’s assessment was to determine whether these policies, procedures and internal controls are sufficient to ensure secure and accurate elections based upon software, hardware, and operational susceptibilities. This Secretary’s Report briefly explains SysTest’s methods and findings. The complete SysTest reports are attached at Appendix G.

### **Method**

- **Representative Sample of Ohio Counties:** The SysTest team reviewed specific procedures in eleven counties (one-eighth of Ohio’s 88 counties) (Allen, Belmont, Cuyahoga, Fairfield, Franklin, Hamilton, Jackson, Licking, Lorain, Montgomery and Warren) as a representative sample of Ohio jurisdictions. These counties were chosen based on size, demographics, and voting systems.
- **Surveys:** Each participating county received written surveys, instructions, and an introductory letter from the secretary of state via hand delivery. Every participating county returned the surveys, and their responses were incorporated into SysTest’s analysis.
- **On-site Interviews and Assessments:** The SysTest team visited each participating county. They assessed each participating county’s facilities, access controls and physical security. They also reviewed election setup, and programming and testing methods for paper and electronic voting systems. The SysTest team discussed Election Day procedures for detecting and resolving machine security and operational issues and the corresponding poll worker training and procedures in each county.
- **Review Vendor Documentation:** The SysTest team also reviewed each participating county’s documentation from its voting system manufacturer. This helped SysTest to assess the level of thoroughness and usability of the documents, particularly as they pertain to security and election accuracy. SysTest also evaluated whether each county’s policies, procedures, and processes implement the vendor’s recommendations.

### **Findings**

#### **Summary**

SysTest concluded that solutions to election administration issues lay not only in technology, but also in management practices, training, and documentation. Summaries of the risks from an elections operations and internal controls perspective are as follows:



1. BOE facilities are not equipped to provide adequate security, storage and access controls for ballots, voting machines, and election systems. This is particularly true after business hours.
2. Oftentimes BOEs do not have written policies and procedures that outline how elections are conducted, voting systems used, and sensitive items secured.
3. Statutes, regulations, and directives do not provide sufficient guidance or they mandate unreasonable or unnecessary timelines. Some of the statutes and regulations are based on outdated voting technology and methods.
4. The bi-partisan system at boards of elections creates inefficient staffing, organizational, and management configurations.

### **Elections Operations and Internal Controls Assessment: Specific Results and Suggested Improvements**

#### **Documentation**

SysTest found common problems among all three manufacturers' documentation. First, SysTest concluded that the level of detail provided in manufacturer documentation was often on a very high level that assumed higher than average technical expertise than BOE employees may have (Final Technical Report at 18.) Second, SysTest found that some of the information provided in the documentation was too complex and did not provide step-by-step procedures. (*Id.*) Therefore, a straightforward task may unnecessarily be turned into a very complex one. As discussed later in this summary, documents should be created for BOE use that contain step-by-step instructions and can be used as a resource guide.

#### **ES&S Documentation**

SysTest found that the ES&S documentation was difficult for boards of elections to use. (*Id.* at 19.) Among the most important findings in the ES&S review was that the documentation could not be used as a quick reference guide. (*Id.*) Specifically, ES&S's Poll Worker Election Day Procedures document is very thorough but includes extraneous and unnecessary information that adds to the level of complexity and confusion. (*Id.*) The ES&S documentation is more oriented toward initial installation and setup rather than ongoing operations. (*Id.* at 20) The emphasis on installation and setup adds to the complexity of the documentation. (*Id.*)

#### **Premier Documentation**

SysTest determined that the Premier documentation is much more structured. (*Id.*) However, the Premier documents also assume a high level of technical knowledge and are organized around technical abilities rather than election functions. (*Id.*) No single document exists for the Premier system that can be used to quickly, efficiently and effectively construct policies, procedures, and processes. (*Id.*) Thus, local election policies, procedures, and processes are pieced from multiple documentation sources.

### Hart InterCivic Documentation

The Hart InterCivic documentation was the most structured according to the SysTest study. (*Id.*) It is broken into various system components and accommodates the nature of election cycles. (*Id.*) It also provides a variety of useful check sheets. (*Id.*) Nonetheless, it is very voluminous and difficult to use quickly. (*Id.*) The documents are not meant to be county-specific. Customizing these documents presupposes a level of technical knowledge that may not be available. (*Id.*)

### **Threat Analysis**

SysTest used a threat model to assess the effectiveness of operational procedures and controls for voting systems in a potentially high-risk environment. (*Id.* at 21.) SysTest also analyzed the types of human threats and their potential actions (*Id.* at 22.) ranging from a nuisance level (level 1) to an inadvertent level (level 2) to a malicious level (level 3). (*Id.* at 29.) SysTest used the concepts of threat deterrence, delay, detection, and denial as its basis for identifying and recommending mitigating measures for the vulnerabilities it identified. (*Id.*) Of those concepts, detection is the most powerful, because it enables state and local election officials to identify, isolate and recover.

Nuisance/level 1 threats are characterized by threats emanating from situations of limited time, access and knowledge. These threats pose a minimal risk and are easily deterred, detected, and isolated. If they occur, they are usually isolated to a single machine or precinct. Mitigation factors are easy, inexpensive and not difficult to implement by local election officials and voting system manufacturers. (*Id.*) Nuisance threats include those initiated by foreign governments, activists, political campaigns, political action committees and organizations, and voters. (*Id.*)

Inadvertent/level 2 threats are the most frequent and likely to occur. They are characterized by lack of training, human error, inadequate quality controls, poor management, and operational, budget, and staffing constraints along with outdated, incomplete or contradictory regulation. (*Id.*) Mitigation strategies for this threat level are typically not technical in nature but require complex action from state and local legislative bodies, elected officials, election officials, and voting system manufacturers. (*Id.*) Inadvertent threats include those from voting system manufacturers, boards of elections staff, poll workers, election-related vendors, and legislation, regulations, and directives, along with election administration and management practices. (*Id.*)

Malicious/level 3 threats are potentially the most disturbing, most intricate to find, and difficult from which to recover. These threats are characterized by authorized access and a high level of technical knowledge. (*Id.* at 30.) Malicious level threats include threats by rogue voting system programmers. Mitigation factors are pointed, expensive, and difficult to implement because the threats are difficult to detect and “global in scale.” (*Id.*) Nonetheless, a parallel testing program of randomly selected voting machines by local election officials and voting system manufacturers could address this situation. (*Id.*)

SysTest notes that it is unrealistic to attempt mitigation strategies that would completely eliminate any and all possible risks without requiring very costly and severe limitations on the right to vote. (*Id.*)

### **Vulnerability Analysis**

SysTest identified eight potential times during the election cycle where threats and threat sources exist in the voting system. (*Id.* at 31.) These times encompass the entire election cycle from pre-election storage, Election Day, and election results and post election storage. (*Id.*) SysTest found that significant internal controls, security measures and operational procedures are in place in the representative counties sampled. (*Id.*) However, the risk potential manifests itself in the absence of formal documentation.

SysTest notes that there are many differences among Ohio counties regarding capabilities, approaches, and resources that disallow uniformity in and among Ohio counties. (*Id.* at 32.)

SysTest identified several potential risk areas in more than one single county independent of voting system, county size and political philosophy. These include:

#### **County Documentation**

SysTest observed that more than one county lacked written documentation of election procedures and security plans. (*Id.* at 34.) Instead of written procedures or staff training, those counties relied upon a single person's knowledge. (*Id.*) This reliance could result in overlooking important practices, inconsistent procedures, and lack of continuity during re-organization or staff turnover. In the event of an election contest court action, this could also raise questions about the staff's personal judgment and decisions. This risk could be mitigated by a comprehensive document developed at the state level covering all elections procedures. (*Id.* at 48.) Counties could then develop county-specific documents.

#### **Physical Security**

SysTest discovered that existing facilities do not provide adequate ballot and voting system protection against unauthorized access. (*Id.* at 34.) SysTest recommends that a physical security and crime prevention assessment be conducted. (*Id.* at 49.) It also recommends that the state develop standard practices for equipment and supplies during transport and storage when equipment is not in control of boards of elections staff members. (*Id.* at 54.) Finally, SysTest opines that contractors that deliver or store equipment should be required to be bonded and insured. (*Id.*)

#### **After Hours Access**

The SysTest report states that while many boards of elections are adequately secured during business hours, most of them are not protected against unauthorized access after business hours because of inadequate key controls, glass paned doors, and ground level windows that are not reinforced. (*Id.* at 35.) However, in some cases, the board of elections has no control over some county facilities where maintenance crews enter at

will. Installing an electronic lock system, a visitor and employee badge system, a video surveillance system or an intrusion detection system could mitigate this risk according to the SysTest report. (*Id.* at 35, 49, 50.)

### Secure Storage

Secure storage areas are inhibited by the facility in which the board of elections is located. Items requiring segregation, secure storage, and inventory controls are co-mingled with less sensitive items. SysTest recommends that a physical security and crime prevention assessment be conducted. (*Id.* at 49.) SysTest also points out that installing an intrusion detection system or video surveillance system could help with this problem. (*Id.* at 49, 50.)

### Two Key/Password Systems

SysTest concluded that the two-key and split password approach regarding access to sensitive areas “provides a false sense of security and may even undermine security for several key reasons.” (*Id.* at 35.) The two key system does not allow anyone to detect someone who accesses the facilities without authorization. (*Id.*) The two key system's effectiveness is also compromised by the ability to duplicate keys, lack of control of the keys, and the ability to leave one of the locks unlocked. The split password system's effectiveness is compromised by the ability and/or inclination to share the password with others for convenience. SysTest suggests that installing an electronic lock system could remedy this issue. (*Id.* at 49.)

### Job Classifications and Hiring Practices/Partisanship

SysTest concluded that partisanship requirements in the Ohio election system imply a mistrust of the opposite party and the expectation that the opposite party is pursuing an advantage for its party. (*Id.* at 36.)

The focus on partisanship requirements may impact whether qualified people are hired that meet the boards' operational and administrative needs. (*Id.*) These requirements also impact the ability to hire and fire, thereby inhibiting management's ability to effectively administer elections and set performance standards. (*Id.*) SysTest further found that political parties control the entire hiring process in some cases. (*Id.*) This could be remedied by a comprehensive document covering all elections procedures developed at the state level (*Id.* at 48) as well as standardized job descriptions that outline minimum job qualifications such as Secretary of State Directive 2007-01, setting qualifications for the hiring of directors and deputy directors of BOEs, and merit based hiring and firing practices (*Id.* at 50.)

### Background Checks

Participating counties reported that, due to partisan requirements, they were unable to perform any type of screening, reference checks, or criminal background checks. (*Id.* at 37.) This subjects boards to the possibility of corrupt insiders or similar accusations. SysTest proposes background checks for permanent employees and temporary employees that handle sensitive information. (*Id.*) Note, the secretary of state obtains criminal background checks and performs a search of any campaign finance law violations before appointing members of boards of elections.

### Systems Integration

Participating counties using the Premier system do not connect their voter registration and election management systems. Such a connection is not available for ES&S or Hart users. Consequently, boards of elections maintain multiple databases requiring double data entry and proofing and synchronization of parallel databases. Election systems not “talking” to each other increases the risk of error. (*Id.*) According to SysTest, manufacturers should “create and/or automate data interfaces that support election management systems and require counties to use them.” (*Id.* at 51.)

## **Election Management Software (EMS) and Firmware Version Control Updates**

### Installation

Participating counties change election management software and voting system firmware using very different methods. Larger counties tend to receive updates and improvements directly from their respective vendors. (*Id.*) Smaller counties, on the other hand, receive updates and improvements through the secretary of state’s field staff personnel. (*Id.*) The SysTest report advises that “standardized and centralized software and firmware” should be installed and a “version protocol” created. (*Id.*) In addition, there should be standardized recordkeeping of current software and firmware versions. (*Id.*)

### Software Chain of Custody and Recordkeeping

The SysTest team did not find any consistent statewide processes regarding how boards of elections should handle introducing, delivering, installing, verifying, testing, controlling and documenting software or firmware changes. (*Id.* at 38.) This is a concern since many opportunities to compromise voting involve unauthorized software and/or firmware. Because there is no local record keeping regarding authorized changes or post-change installation testing, board of elections personnel rely completely on their vendors to validate any changes or updates. (*Id.*) SysTest recommends that the State take over that responsibility. (*Id.*)

### Certification of the Ballot

Many time-sensitive tasks are dependent upon ballot finalization and certification. The Ohio Revised Code requires the secretary of state to certify ballots 60 days before Election Day. SysTest recommends that the secretary of state strictly adhere to this timeline to prevent down-stream implications as well as review and seek or implement changes to statutes, regulations, and directives so that they conform to new technology, time constraints, and timelines. (*Id.*)

### Marking of Test Ballots

Logic and accuracy testing (“L&A” testing) is designed to ensure that all ballot layouts can be accurately read, that all ballot positions can be accurately and reliably voted, and

that the ballots will be read correctly. However, the approach toward L&A testing is apparently still based on out-of-date punch card testing and is not designed to catch mistakes unique to optical scan or electronic voting. (*Id.* at 39.) SysTest proposes conducting L&A testing using hand marked ballots and counting a representative sample of test ballots. (*Id.*) Moreover, standardized L&A testing should be conducted at the state level to “include a complete end to end battery of tests of individual machines, and central count systems.” (*Id.*)

### Testing Scenarios

Boards of election have relied upon oral history regarding testing practices rather than developing system-specific documents that outline proofing/testing timelines, criteria, and methodology. (*Id.*) Such documents would avoid chaos when staff turns over and increase the counties’ ability to detect and correct errors.

### Absentee Ballots

Recent changes to Ohio law provide for no-excuse absentee voting, an option that is becoming increasingly popular with each election. SysTest found that the procedures for issuing, handling, tabulating, and reconciling absentee ballots are not in line with legal and voting technology changes. (*Id.* at 40.) SysTest makes several recommendations regarding how to bring these practices up to date, including creating consistent absentee ballot stub number policies, and processing absentee ballots before Election Day to accommodate volume and clear directions regarding the process. (*Id.*) SysTest further recommends prioritizing absentee ballot post election reconciliation and creating consistent procedures regarding exceptions to the handling, ballot duplication, and enhancement processes. (*Id.*) Each exception should be documented. (*Id.*) BOEs should further create procedures for elections personnel and volunteers to vote absentee. (*Id.*) SysTest also encourages that the state review and revise absentee ballot statutes, regulations and directives to make them conform to current technology and voting practices. (*Id.* at 53.)

### Inventories

SysTest survey results and onsite visits showed that counties do not have verified serial number inventories or a method to account for or mark memory cards on an ongoing basis. (*Id.*) Memory cards contain ballots that must be retained according to federal or state record retention schedules. SysTest recommends that the state establish standard inventory controls. (*Id.* at 54.)

### Security seals

Boards of elections’ security seal practices generally provided the requisite security. However, SysTest recommends implementing uniform procedures instructing poll workers to check for the presence of the seals and verify the serial number before machine operation. (*Id.* at 41, 42.)

### Poll Worker Training

Due to recent changes in election law and lawsuits related to these changes, there is a wide-variety of election law interpretations among Ohio’s county boards of elections.

Adding to this challenge is the large amount of poll worker turnover. The SysTest report emphasized the need for uniform policies, procedures, and processes for poll workers that take into account each type of voting system. (*Id.* at 42.) SysTest further recommends that Ohio conduct vigorous poll worker training and test whether each poll worker understands the material and can execute it. (*Id.* at 42, 54.) SysTest states that making all poll workers experts in every area of elections is not practical. (*Id.* at 42.) Instead, SysTest suggests that poll workers be trained on prioritized topics and that class time be reduced. (*Id.* at 42, 54.)

### Second Chance Voting

Optical scan systems notify voters if they have under- or overvoted and give them a second chance to correct the under- or overvote. A voter can use an over-ride function to ignore these warnings. Some counties place these ballots in a bin for processing by poll workers after the voters leave. (*Id.* at 42.) SysTest suggests that the over-ride function be left to each voter. (*Id.* at 42-43.) SysTest also recommends that the state review and revise absentee ballot statutes, regulations and directives to make them conform to current technology and voting practices. (*Id.* at 53.) Standard criteria should be developed for handling second chance voting on precinct count optical scan equipment also. (*Id.* at 42.)

### Multi-Precinct Polling Locations

The majority of counties allocate several precincts to common polling locations for accessibility and efficiency. Usually, each machine in the polling location is programmed with ballots for all precincts assigned to that polling location rather than a voting machine's ballots being precinct specific. This way, voters can use any machine in the polling place. SysTest recommends that statutes and directives should recognize and develop standards for this process. (*Id.* at 55.)

### Issuing Provisional Ballots

Provisional voting sometimes creates long lines, making it difficult to manage lines and the flow of voters. Few boards of elections have processes in place to deal with this issue. (*Id.* at 43.) This issue can be lessened by developing procedures that identify provisional voters early and that take them aside to allow them to vote. (*Id.* at 43-44.)

### Two-Person Rule

On election night the presiding judge returns voted ballots to the board of elections or to a designated drop station. Once the board of elections staffs receives the ballot, the two-person rule dictating that a Republican and Democrat handle ballots at the same time is employed. SysTest notes that there is a greater risk of tampering when the ballots are in the presiding judge's custody alone. (*Id.* at 44.)

### Reconciliation/Canvassing

SysTest observed counties using punch card, paper ballot and single voting system assumptions for canvassing election returns. (*Id.*) These processes do not always sufficiently audit electronic voting for multi-precinct polling locations. Absentee ballots are not audited as robustly as poll ballots and at times are not reconciled at all. (*Id.*) A

lack of understanding of auditing and canvassing principles and the absence of written documentation leads to partial and inadequate post election checks and balances. SysTest recommends establishing standards for canvassing, auditing, and reconciling election returns that consider all voting systems, technologies, and ballot types. (*Id.* at 55.) They further suggest that voted paper ballot security and transportation rules be clarified. (*Id.*)

#### Qualification of Provisional Ballots

Provisional ballots are generally processed just after Election Day. However, SysTest notes that checks for double voting were weak, did not exist, or were done manually. (*Id.* at 44-45.) Absentee ballot checks, in contrast, were more thorough and automated. (*Id.*) Additionally, some counties tally and report provisional ballots in such a way that could compromise voter confidentiality. (*Id.* at 44.) SysTest recommends standardizing requirements and procedures for processing provisional ballots. (*Id.* at 56.)

#### Canvass Discrepancies

None of the counties had formalized written procedures to track, document or report discrepancies discovered during the canvass process. (*Id.* at 45.) This could be resolved with written documentation regarding the canvass process. (*Id.* at 45, 56.) This document, SysTest counsels, should address discrepancies found in the canvass, research conducted to find the root of the discrepancy, corrective actions taken, the impact of unresolved discrepancies, and preventive actions taken. (*Id.* at 45.) This document should be a public record presented to each board member. (*Id.*)

### **Summary of Boards of Elections Officials' Review of SysTest's Findings on the Elections Operations and Internal Controls Assessment of the State's Voting Systems**

One Republican and one Democrat boards of elections official each reviewed SysTest's findings on the election operations and internal controls of Ohio's three voting systems. Both of these officials utilize the Premier DRE voting system in their respective counties. In addition to the elections officials, the review group consisted of three secretary of state employees — a facilitator, an attorney, and a "scribe." A "Capsule Summary Statement" of the elections officials' review is provided below, basically as prepared by the "scribe," along with a table summarizing this boards of elections review team's standardized evaluation of SysTest's findings.

#### **Capsule Summary Statement by Boards of Elections Team Reviewing SysTest's Findings on Elections Operations and Internal Controls**

The election officials found the SysTest assessment of elections operations and internal controls credible. The election officials felt the strongest component of the report's credibility stemmed from its reliance on actual information from 11 of Ohio's boards of elections. The four main areas covered in this report called for stronger training and education, written policies and procedures, documentation, and standardization or



centralization.

While the election officials review team found this report credible, there were disagreements with some the report's conclusions. For example, the review team strongly disagrees with the conclusion that Ohio's bipartisan elections system should be eliminated. The review team also expressed some concerns with the levels of threat or risk indicated without having more quantifiable examples of their incidence.

The election officials agreed with the report that there exists a need for more standardization from the office of the secretary of state. The election officials believe that, regardless of which voting system is used and how reliable it may be, without standard procedures and policies greater risk will continue to exist.

**Summary Table of Standardized Evaluations by Board of Elections Team Reviewing SysTest's Findings on Elections Operations and Internal Controls**

**Average Operational Controls Report Quality Ratings by Election Officials**

Quality	Scale	Overall
Data	1-3	2.0
Claims	1-3	2.0
Warrants	1-4	2.5
Coherence	1-4	3.0
Overall	1-5	4.0

Note. This table represents the average ratings of two election officials

**Report Quality Rating Scales**

Scale	Dimension Measured
Data	Conclusions were based on and supported by data.
Claims	Claims were clear, consistent, feasible, and related to solutions
Warrants	Arguments were reliable, trustworthy, and logical
Coherence	Material was integrated and contained sufficient context
Overall	Overall report quality from failing to excellent

## **Secretary of State Recommendations**

### **General Conclusions and Background**

The findings of the various scientists engaged by Project EVEREST are disturbing. These findings do not lend themselves to sustained or increased confidence in Ohio's voting systems. The findings appearing in the reports necessitate that Ohio's voting process be modified to eliminate as many known risks to voting integrity as possible while keeping voting accessible to Ohio's voters. These changes must be thoughtfully planned with the assistance of the Ohio General Assembly, Governor Strickland and Ohio's election officials. As they are implemented, these changes must be made widely known to the public to facilitate orderly and cost efficient implementation.

As Ohio's voting system is restructured, all equipment and any related software, along with software updates, must be documented in a central registry to ensure that all equipment and software in use has been certified by the state's Board of Voting Machine Examiners. Preparation, use and storage of equipment before, during and after an Election Day must be supported by uniform guidelines, procedures and training supplied by a combination of legislation and secretary of state directives.

It has been said that elections belong to the people. Excessive dependence on any voting machine company to operate the state's elections, when that company's voting system is subject to trade secret or propriety information claims, results in a loss of transparency that should exist to assure election officials and the public that a fair and accurate process has been implemented for democratic self-governance. The information utilized by the scientists in this study included reviews of all three systems' software source codes and related documentation, a thorough orientation to the operation and use of the machines, other system documentation and a review of previous reports of risk assessment of similar voting systems performed by other states and institutions. The information available to the scientists who performed the assessments of this study is some of the most comprehensive information available to date for any such study. This was not accomplished without the assistance and cooperation of the voting machine companies whose equipment and software were studied.

It should be noted that, in cooperative discussions with the voting machine companies, it is already recognized by one or more of them that problems exist with systems now in operation in Ohio and elsewhere in the U.S. Upgraded software and hardware is being tested for federal certification, which could replace equipment and software now in use in Ohio. Originally, two of the voting machine companies—Premier Election Solutions and ES&S—had requested that the secretary of state assess as part of Project EVEREST their “next generation” systems. Unfortunately, testing for federal certification of these proposed system solutions was not completed in time for it to be assessed as a part of this study. It is not known whether the “next generation” systems will diminish the risks found by the scientists in this study. Additional, similar testing is warranted, especially as it relates to server software for ballot design and vote tabulation.

All systems studied in Project EVEREST utilize for each county a central server and software for ballot definition and vote tabulation, and in some instances computer

workstations connected to the central server to extend the number of users of the server in preparing for or tabulating an election. Memory cards are the prime method used to transmit ballot definitions from the server or workstations to precinct-based machines and from the precinct-based machines to the server for vote tabulation. The precinct-based machines are either electronic machines that allow for marking ballot selections by either a touch screen or a dial and ballot optical scanners for scanning hand- or machine-marked votes on paper ballots, such as provisional and absentee ballots and some ballots marked by voters with disabilities. This system of voting is, in simple terms, computer-based voting.

Computers are widely used in our society for communication, financial transactions, complex problem solving and other functions requiring timeliness, accuracy and efficiency. Standards exist in the computer industry for requisite levels of security to protect privacy, integrity of methodology, and accuracy of data. It would follow that computers can be used to enhance the voting experience and should be subject to industry security standards as are other computer-based applications.

Unfortunately, the findings in this study indicate that the computer-based voting systems in use in Ohio do not meet computer industry security standards and are susceptible to breaches of security that may jeopardize the integrity of the voting process. Such safeguards were neither required by federal regulatory authorities, nor voluntarily applied to their systems by voting machine companies, as these products were certified for use in federal and state elections.

With Ohio's historical role in presidential elections and the 2008 presidential election fast approaching, the integrity of the state's voting process is of paramount importance. Ohio's voting system must be reliable and accurate to ensure fair results and voter confidence. It is discouraging that public funds have been spent not just in Ohio, but also nationally, for computer-based voting software that is antiquated, underdeveloped from a security standpoint, and in many cases, unstable. Much of today's current situation has evolved from a combination of 1) the unrealistic expectations of the tide of change following the 2000 presidential election seeking quick solutions for better, more reliable voting systems when the underbelly of the punch card election system was exposed in a close presidential popular vote, 2) the opportunities presented by this tide of change for voting machine companies to sell mass quantities of voting machines to state governments all over the nation, resulting in less than optimum research and design of the security of computer software and system configurations, 3) the failure of Congress and/or its newly established regulatory agency, the Election Assistance Commission, to recognize that computer-based voting, heavily marketed as a panacea, should be subject to stringent security testing to ensure it meets computer security industry standards, and 4) the failure of Congress to fully fund the Help America Vote Act by approximately \$800 million dollars to provide for adequate funding of the Election Assistance Commission and for training and other implementation solutions for the states.

While the advisory group of the state's election officials generally found that many of the scenarios described by corporate and academic security scientists may not be regularly anticipated in a "real-life" setting, the fact that no safeguards have been built into the state's voting systems to ensure that they do not occur is disconcerting and serves to undermine voter confidence. When HAVA was implemented in Ohio, the state provided little or no step-by-step guidance to county boards of elections. This left them

in a “thrown to the wolves” position to work with voting machine companies and their service technicians in implementing the new, computer-based systems or to develop their own procedures for implementing these systems in compliance with federal and state law, the latter of which contains gaps and provisions no longer consistent with the new voting machine technology. Election officials, being resourceful, persistent and adaptable, implemented this new generation of voting equipment and software under these less than optimum conditions and, in many cases, without guidance from the state. Complicating this is the state’s structure for funding elections, with directives coming from state and federal sources, but funding coming from the local board of county commissioners. All of this has resulted in a garden variety of procedures from county-to-county in Ohio, not all of which provide to each Ohioan the same level of ease or protection of the voting franchise.

Conscientious elections officials, who work many hours to prepare for an election and take seriously their role in ensuring a fair and efficient process, were placed in precarious positions, resulting in many of them “throwing in the towel” after many years of service and retiring or leaving the field of election administration. Staff turnover, and often with it, the loss of years of experience and knowledge, coupled with a lack of documentation or documentation no longer applicable to new voting procedures, has contributed to confusion and turmoil in the administration of elections.

The term “elections professional” has emerged, with training conferences and organizations often funded in part by voting machine companies resulting in an inevitable blurring of the distinctions between being an expert at ensuring a competent and responsive election process and being an expert at handling computer-based voting machines. This may account, in part, for the reluctance of some proficient election officials to scrutinize the security or integrity of computer-based voting systems. It has fed the accusations by voting protection activists that elections officials and voting machine companies share a common purpose. Such grassroots voting protection activism developed after a voting machine company chief executive from Ohio expressed in writing his intention to deliver the state for a particular presidential candidate in 2004—an incident that has been described as a “nuclear moment.”

In this environment Project EVEREST was conceived and undertaken in Ohio, a state at the root of election controversy, by a new secretary of state administration, to keep a promise to conduct a top-to-bottom review of its voting systems. The study’s purpose is and has been to gain information about the integrity of Ohio’s voting process and, more specifically, to assess risks associated with the state’s voting systems to ultimately strengthen voter confidence in Ohio and the confidence of the nation in Ohio’s voting process. While the initial reaction may be that the study’s findings do not instill confidence, the recommendations contained in this report will allow Ohio to move forward toward meeting Ohio voter expectations for elections that are safe, reliable and trustworthy and that merit the nation’s confidence in its outcomes.

The results of the study point to the need for great change not just in Ohio, but also in voting systems and procedures used in federal elections in general. The recommendations of this report were developed in consultation with an advisory group of twelve (12) elections officials from throughout Ohio with geographic and voting machine diversity, and whose numbers totaled six (6) Democrats and (6) Republicans, all of whom are directors or deputy directors of boards of elections with collective decades of experience. While not all elections officials have fully embraced all aspects of

these recommendations, all have expressed their willingness to assist in their implementation if Governor Strickland and the Ohio General Assembly agree that they should be implemented in whole or in part. For this, the secretary of state expresses gratefulness and respect.

## **Recommendations**

### ***Introduction***

In reviewing the findings of the various scientists of the study, the secretary of state finds that no system used in Ohio is without significant and serious risks to voting integrity. This appears to be a problem inherent with the products in use throughout the country as supplied by the industry. The Ohio secretary of state is constrained by the existence of available resources and necessarily makes some recommendations that security experts may consider less than optimum but that pose fewer risks than continuing to use the system as currently configured and implemented.

At present, Ohioans vote on Election Day at localized polling locations and, before the election, at boards of elections. Ballots are organized according to precincts comprised of no more than 1400 electors. Voting occurs on Election Day from 6:30 a.m. to 7:30 p.m., while early voting (as an in-person form of absentee voting) takes place during regular hours of boards of elections from thirty-five (35) days before the election through the day before Election Day.

Absentee voting by mail takes place beginning thirty-five (35) days before Election Day, and all ballots must be received no later than Election Day, except for military and overseas absentee ballots, which must be postmarked no later than Election Day and received no later than ten (10) days after the election. Provisional voting generally takes place on Election Day by voters who do not supply the preferred methods of identification (photo ID issued by the state or federal government, utility bill, bank statement, paycheck or government check or other government document) and by voters appearing at a polling location whose address does not match the address recorded in the poll book at that polling location or whose name does not appear in the poll book. Regardless of type of voting system used in a county, provisional ballots are paper ballots by virtue of a recent directive issued by the secretary of state (as a result of limitations of the VVPAT, “voter verified paper audit trail” in identifying provisional ballots ultimately as belonging to a particular voter) to ease the process of recounts and protect ballot secrecy for each voter.

## **Recommendations**

### ***Recommendation #1 – Eliminate points of entry creating unnecessary voting system risk by moving to Central Counting of Ballots***

The computer-based voting systems (all three of them) used in Ohio transmit ballot definition and votes for tabulation on memory cards (and in some cases on peripheral coding devices). These cards and devices are insecure and operated in environments where there are many levels of access to these devices (voters, poll workers, election officials, contractors and vendor representatives). These devices are used in multiple ports of entry to the system and shared between various components of

the system, whose shared data travels to the ultimate destination of the server software used for present and future elections. Accordingly, the prudent course of action is to remove insecure ports of entry to the system from less secure environments such as polling locations.

**Recommendation #2 – Eliminate DREs and Precinct-based Optical Scan Voting Machines that tabulate votes at polling locations**

Simply put, the elimination from polling locations of vote recording and tabulation machines such as DREs and precinct-based optical scan machines (except to use optical scan machines for determining overvotes and undervotes to satisfy HAVA “second chance” requirements) and instead migrating to central counting of ballots, ensures greater stability to the computer-based voting systems, because it eliminates multiple points of entry to a system not adequately secured.

**Recommendation #3 – Utilize the AutoMark for voters with disabilities**

The only computer-based system operated at the precinct level that does not tabulate votes is the AutoMark voting machine. This machine “reads” the bar code on a blank ballot using preprogrammed firmware and acts solely as a ballot marking device, allowing voters, especially those with disabilities, to mark their ballots with little or no assistance, preserving the secrecy of their ballot selections. The marked ballot is ejected once voted, and the voter places the voted ballot into a ballot box or scanner along with all other optical scan ballots. AutoMark voting machines should be used at all polling locations for voters who need assistance marking their ballots and for voters wishing to cast their ballots via a touch screen method.

**Recommendation #4 – Require all ballots be Optical Scan Ballots for central tabulation and effective voter verification**

As noted above, optical scan ballots provide greater opportunities for voter verification and are the only type of paper ballot able to be centrally counted with current technology. They are compatible with the non-tabulating AutoMark voting machine, effective for voters needing assistance. Optical scan voting is currently used in polling locations in approximately twenty-nine (29) counties. Optical scan ballots are consistent with provisional and absentee ballots already in use. Counties currently using DRE technology must still use optical scan ballots for absentee and provisional voting. With a movement to optical scan voting, ballots in a county would be of the same type and counted by high speed optical scanners (or by formerly precinct-based optical scanners centrally located as an interim measure.) Legislation would be needed to allow printing of ballots by printers from outside the State of Ohio to accommodate the increased volume of ballots to be printed.

**Recommendation #5 – Maintain “no fault” absentee voting while establishing Early (15 days prior to the election) and Election Day Vote Centers (of the size of 5 to 10 precincts), eliminating voting at individual precincts or polling places of less than 5 precincts**

“No fault” absentee voting (voting absentee without a stated reason), adopted in 2005, should be maintained to encourage participation while thinning Election Day voting. “Early voting” currently occurs as an “in-person” form of absentee voting,

requiring the voter to complete an absentee ballot application onsite when he or she appears at a board of elections to vote during the absentee balloting period. Voting at boards of elections by in-person absentee ballot would begin at the inception of the 35-day absentee voting period prior to an election, but at the 15-day point, additional voter centers would open for continuous voting seven (7) days per week through Election Day. On Election Day, vote centers would be open during traditional voting hours—6:30 a.m. through 7:30 p.m. On the days during the 15-day early voting period, vote centers (including boards of elections) would be open from 7:00 a.m. through 7:00 p.m. Monday through Saturday and from 12:00 noon through 7:00 p.m. on Sundays, staffed by two shifts of seven (7) hours each with an hour overlap during the period of 12:30 p.m. to 1:30 p.m. on Mondays through Saturdays. Voters would be assigned to a particular vote center as their polling location. Examples of vote centers would include libraries, community centers, senior centers, shopping centers or other accessible public buildings with adequate parking. Precincts would be maintained in the board's records, but vote centers would be created for 5 to 10 precincts, with extra staffing and materials planned for Election Day, especially in the first few years.

Ballots would be pre-printed optical scan ballots, and each polling place would maintain a separate ballot box for each election precinct. Voted ballots would be placed in the appropriate precinct box and returned in the box unopened or sealed for secrecy at the end of each day to the board of elections. Procedures would be prescribed by directive and/or statute for daily ballot reconciliations and with daily poll lists and poll books transported to the voter center each day. On Election Day, a mid-day pickup of ballots by board personnel would need to be authorized by legislation to permit scanning (not tabulation) before 7:30 p.m. on Election Day. Vote centers would also be equipped with two AutoMark ballot marking devices for voters with disabilities or needing assistance or who wished to use touchscreen and with two precinct-based optical scan machines for voters who wish to check their ballots for overvotes or undervotes by scanning them (with no tabulation occurring, but some firmware needed to read ballots to detect overvotes or undervotes). Voters would be able to drop off absentee ballots at vote centers for return to boards of elections. Early voting at vote centers may reduce the number of provisional ballots and provide more time to verify information for provisional ballots. Adequate signage and voter education would also need to be conducted to inform voters of 1) the availability of early voting in multiple locations, 2) the change to vote centers on Election Day, and 3) the need to carefully check ballots to ensure they have been correctly voted, avoiding overvotes or undervotes.

Other equipment needed for polling places would include privacy booths with surfaces for voting optical scan ballots, marking devices such as pens or pencils, extension cords for AutoMark machines, and optional storage for election related equipment and supplies. Any ballots stored at vote centers would need to meet standardized security requirements set by directive or statute. Otherwise, ballots would be delivered to vote centers daily. All ballots would be serialized for reconciliation purposes and all voted ballots would be returned to the board of elections at the end of each voting day.

After piloting the vote center/early voting concept in 2 or 3 counties at the March 2008 primary election (see Recommendation #7 below), vote centers and centralized optical scan voting would be implemented in the November 2008 election, as long as funding is available by mid-April 2008. Funding would be for the 2008 general election only and would include the following:

1. Funding for vote center workers exceeding what is already budgeted for paying poll workers in the November 2008 election (per county). Suggested minimum rate of pay is the state minimum wage of \$6.85 per hour, allowing counties to adjust upward for differing wage rates around the state;
2. Funding for printing optical scan ballots above what is already budgeted for November 2008 election (per county). Note some counties already have budgeted the printing of optical scan ballots for the entire county, since they are already using optical scan ballots;
3. Funding for high-speed optical scan machines (at present only one voting machine company has a certified high-speed optical scan machine, but several other vendors are awaiting certification of high speed optical scan machines, which would likely be available for certification by the Board of Voting Machine Examiners and for sale in Ohio by April 2008). Some counties already have high-speed optical scan machines, and the secretary of state has an inventory record of what is already on hand;
4. Funding for voting booths for use with voting optical scan ballots. Some counties retained their voting booths for punch card voting, and some of these may be converted for optical scan voting for a cost less than purchasing new ones. Other counties currently using optical scan that moved from precinct based voting to vote center voting would have extra voting booths. Those purchased with federal HAVA dollars could be redistributed, and those purchased with county funds could be purchased at resale cost;
5. Funding for purchase of ballot boxes for daily transport of voted ballots from vote centers to the board of elections;
6. Funding for leases of space for vote centers in excess of what is already budgeted for leases for polling places for November 2008;
7. AutoMark precinct-based ballot marking devices purchased with federal HAVA dollars could be redistributed among vote centers from counties using them in each precinct or polling location, with funding necessary to pay only for machines or accessories purchased with county funds, but at resale cost;
8. Already existing precinct-based optical scan machines purchased with federal HAVA dollars could be redistributed among vote centers (to satisfy second-chance voting requirements) from counties using them in each precinct or polling location, with funding necessary to pay only for machines or accessories purchased with county funds, but at resale cost;
9. Funding for software and/or servers compatible with high speed scanners purchased for central tabulation of optical scan ballots; and



10. Funding for public education about the changes to vote centers and second chance voting where precinct-based optical scanners may not be in use to scan for overvotes and undervotes.

***Recommendation #6 – require all Special Elections (issues only) held in August 2008 to be voted by mail (no in-person voting, except at the board of elections, for issue-only elections held in August 2008)***

Adopt either Sen. Cates' bill (S.B. 182) or similar legislation to require all-absentee voting for special elections (issues-only) as an interim step to all-mail special elections (issues-only). Eventually eliminate the required step of applying for an absentee ballot and simply mail ballots to all electors eligible to vote on the issue(s) submitted to the electorate.

***Recommendation #7 – implement Pilot Programs for vote centers at the March 2008 election in 2 to 3 counties already using optical scan voting***

Allow 2 to 3 counties already utilizing optical scan voting to voluntarily implement Pilot Programs for Vote Centers in the March 2008 presidential primary election and evaluate specific features and practices for improved future implementation, however, being poised to implement them statewide for the November 2008 election.

***Recommendation #8 – adopt legislation to allow a county to vote on whether it desires to vote by mail for a temporary or permanent period of time (see, R.C. 3506.02 for amendment).***

Such an election could take place on a pilot basis at the August 2008 special election. Voters in a county could specify if they wanted mail-in voting and whether it would be solely by absentee vote or by regular ballots mailed to all registered electors in the county. The mail-in voting could be for a specific trial period or indefinitely, depending on legislative preference.

***Recommendation #9 – for the March 2008 primary election permit county boards of elections using precinct-based optical scan machines to move the machines to a central location to implement centralized counting of optical scan ballots***

Counties exercising this option could opt to move to high speed optical scanners for the November 2008 election with available funding.

***Recommendation #10 – for the March 2008 primary election require counties utilizing DREs to offer paper ballots to voters who do not want to vote on DREs***

At the date of this report, it would be extremely difficult for all Ohio counties currently using DREs (a total of 58 counties) to move to a central count optical scan system before the March 2008 primary election. For counties that find themselves in a position of needing to conduct the March 2008 primary election utilizing DREs for voting, electors should be provided the option to vote a paper optical scan ballot at their

polling places. This may be accomplished by legislation. The secretary of state should provide by directive (as opposed to legislation) a temporary determination (specific to the March 2008 election) of the number of optical scan ballots counties should print for distribution upon request in voting precincts where DREs are still in use. The secretary of state is willing to confer with legislative leaders, the Ohio Association of Election Officials and the Ohio Association of County Commissioners on appropriate levels of these substitute paper ballots for the March 2008 primary election. Ballot boxes and secrecy envelopes would also need to be purchased, in addition to voting booths for marking optical scan ballots. These could be used in the fall election for vote centers.

### **Other Options**

The advisory group of 12 election officials discussed earlier assisted in the development of the recommendations listed above. Not all were enthusiastic about eliminating DREs but all expressed willingness to assist at every stage of planning and implementation of any or all of these recommendations.

Other options explored but deemed to be more costly include the following:

#### ***Central Count Optical Scan Voting at Regular Precinct/Polling Locations using AutoMark for Voters with Disabilities***

1. Continue with precinct or polling place based voting using central count optical scan machines, with second chance provided by advertising as permitted by HAVA and utilizing AutoMark ballot marking devices for voters with disabilities. Potential problems with this option include the perennial challenge of recruiting enough poll workers, although training is simpler without DREs or precinct based optical scan machines. In addition, more AutoMark machines would need to be purchased at a per-unit price of approximately \$5400, and this adds significantly to the cost.

#### ***Vote by Mail***

2. Eliminate in-person voting, except in case of voters with disabilities using AutoMark machines. All registered electors would receive a regular ballot by mail. Potential problems with this option include ensuring the integrity of county voter databases that should avoid (but do not always avoid) duplications. Voter ID requirements would more likely ensure honesty in voted ballots (i.e. actually voted by the named voter). This is a more expensive option, especially if the ballot is several pages. It is anticipated that return postage would need to be paid, but "drop off boxes" at specific locations could be utilized to avoid return postage. The State of Oregon successfully utilizes this method, along with nearly all counties in the State of Washington. Voter participation is shown to be higher with this method. This could be piloted at the November 2008 election at a county's option (see Recommendation #8 and R.C. 3506.02 and potential to amend this section).

#### ***Move back the 2008 Primary Election Date to Implement More Recommendations Sooner***

3. This option may allow for the implementation of more recommendations sooner; for more pilot experiments before the November 2008 general election; and for some counties to discontinue DRE use and move to optical scan for the primary. However, delays in funding past, for instance, a first Tuesday after the first Monday in May date could make November implementation difficult if only pilot programs are attempted in May or if funding for changes in November is not determined until after a May primary. Moreover, political and primary election logistical problems could arise in moving back the primary election date, because candidate planning, petition circulation and even filing may already have begun. This would appear to be an option of lesser attraction for all of these reasons.

### ***Cuyahoga County Primary Election Remedy***

4. Software problems associated with Cuyahoga County's GEMS server for its DRE-based voting system occurred at the November 2007 election. Because that election involved a turnout of approximately 15%, and turnout is expected to be substantially higher in March 2008, great concern exists for continued use of this voting system in Cuyahoga County in the March 2008 primary. With the state's funding assistance, Cuyahoga County could move to a central-count optical scan system for the March 2008 primary election by utilizing leased DREs for precinct based voting by persons with disabilities and purchasing high speed optical scanners (with compatible server and software and voting booths) for optical scan voting. This option has been estimated to cost between \$2 million and \$2.5 million dollars. All purchased equipment could transfer to a vote center voting system for use in November 2008, and extra voting booths not needed for vote centers could be redistributed to other counties migrating from DRE to optical scan central count vote centers. The county would be responsible for printing a sufficient number of ballots for the March primary election. If this option is approved, purchases would need to be made immediately, with reimbursement applied for by the secretary of state to the Ohio General Assembly to reimburse the Cuyahoga County Commissioners for equipment purchases.

### **Other Legislation and/or Directives or Rules to be Implemented as a Result of Findings**

Following is a list of other legislation and/or directives or rules not specifically mentioned in the Recommendations above but that are recommended to be implemented as a result of the study's findings. This list is not exhaustive, especially as to directives that will be needed to implement some or all of the above Recommendations:

1. Clarify the law to ensure that vendors and boards of elections notify the secretary of state when "enhancements" and "significant adjustments" are made to the hardware and software. Also, include "firmware" as part of the identified items. (LEGISLATION);
2. Adequately and more frequently train poll workers and presiding judges. (Requires changes to R.C. 3501.27) (LEGISLATION);

3. Require a standard quality of paper and method of handling for the Voter Verified Paper Audit Trail (VVPAT) as a temporary measure for the 2008 primary election. (DIRECTIVE);
4. Reduce the amount of necessary information required on the official ballot to decrease the number of pages of a ballot, including exploring using a “key-type ballot” for voting on issues, with a less expensively printed explanation of the issues. (Requires changes to R.C. 3513.052 & 3513.30) (LEGISLATION);
5. Establish set procedures for the distribution of electronic voting machines. This proposal would allow the secretary of state to define, using specified variables, how many machines should be allocated for each precinct for the March 2008 primary election. (R.C. 3501.11 (I)) (LEGISLATION OR DIRECTIVE);
6. Expand the “Youth at the Booth” program to allow up to 2 high school seniors to serve as poll workers (for early voting at vote centers and) on Election Day and to allow college students to serve in the county where they attend school. (Requires change to R.C. 3501.22(C)) See also, H.B. 350. (LEGISLATION);
7. Change or remove sections of the Ohio Revised Code that are out-dated and/or inconsistent with technology and related procedures. (Ohio Association of Election Officials has been compiling a list.) (LEGISLATION);
8. Permit absentee ballots that are postmarked on or before Election Day to be counted if received by the board of elections within 10 days of Election Day (see Rep. Dyer’s bill, H.B. 336). (LEGISLATION);
9. Permit absentee ballots to be counted if the identification envelope is missing information that was supplied on the absentee ballot application that does not prevent the board of elections from identifying the voter. (LEGISLATION);
10. Permit boards of elections to accept faxed absentee ballot applications. (R.C. 3509.03) (LEGISLATION);
11. Permit permanent absentee status for stated situations, e.g. permanently disabled, no longer have a driver’s license or of a certain age. (LEGISLATION);
12. Make absentee ballot return envelopes significantly distinguishable from regular mail so as to make it easily identifiable by United States Postal Service workers. (DIRECTIVE OR RULE);
13. Permit and require the certification of electronic poll books. (R.C. 3505.05) (LEGISLATION);
14. Establish security protocols for election servers and software. (DIRECTIVE OR RULE);

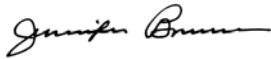
15. Specify standards for Logic and Accuracy (L&A) testing of tabulating machines. (DIRECTIVE OR RULE, POSSIBLY LEGISLATION); and
16. Establish standardized security procedures based on specified levels of risk for components of voting systems. (DIRECTIVE OR RULE).

## **Conclusion**

The implications of this report are serious. Swift and specific changes are needed to improve the quality of Ohio elections so that Ohio is prepared to successfully execute next year's presidential election. Ohio election officials have shown an eagerness to participate in the planning and implementation of these needed changes, and the secretary of state looks forward to working with them and the Ohio legislature in achieving these needed improvements.

The secretary of state is grateful for the stated intentions of Governor Strickland and leaders of the Ohio General Assembly to work in a bipartisan fashion to resolve issues affecting election integrity and to make Ohio a model for other states in implementing election reform.

Sincerely,



Jennifer Brunner  
Ohio Secretary of State



**JENNIFER BRUNNER**  
**OHIO SECRETARY OF STATE**

180 EAST BROAD STREET  
COLUMBUS, OHIO 43215  
TELEPHONE: 614-466-3613  
TOLL-FREE: 877-767-3453  
[WWW.SOS.STATE.OH.US](http://WWW.SOS.STATE.OH.US)  
[JBRUNNER@SOS.STATE.OH.US](mailto:JBRUNNER@SOS.STATE.OH.US)