Ohio Secretary of State J. Kenneth Blackwell

Ohio Secretary of State
DRE Security Assessment

Volume 1
Computerized Voting Systems
Security Assessment:
Summary of Findings and Recommendations

21 November 2003

InfoSENTRY Services, Inc.
www.infosentry.com
919.838.8570

Table of Contents

Introduction and Background

A change in United States election reform that began in the 1960s gained significant momentum in 2002 when Congress passed the Help America Vote Act (HAVA). In the mid-60s, the President and Congress took a major step toward placement of Federal mandates on voting with passage of the landmark Voting Rights Act. While the act had theoretical limitations to certain states and portions of states, its ramifications were national in scope. The message was that the Federal Government considered voting to be so central to democracy in the country that national policies should be established to assure equal rights to the ballot box.

After almost two decades of litigation and congressional action on voting rights issues, Congress passed and another president signed the National Voter Registration Act (NVRA) in the early 1990s. This legislation extended federal requirements to voter registration and took one additional, important step in changing the relationship between local, state, and Federal administration of elections. It mandated naming of a Chief State Election Official in the states. While a few states fall outside NVRA's requirements, there was a new position in the states with expectations that it at least coordinate state and local election activities.

The passage of the Help America Vote Act in 2002 "closed the loop" further by mandating new responsibilities and authority for the Chief State Election Officials. HAVA appears to place the Chief State Election Official in a much more central role of election administration and **management** in the states. The position of Chief State Election Official has three attributes that were not present before: (1) statutory authority granted by the Federal government and state governments to carry out and regulate election administration and management activities, (2) statutory responsibility to see that their respective states meet HAVA's election and voting systems requirements, and (3) funds from the Federal government to meet their responsibilities.

Arguments persist as to the exact nature of the authority and responsibility. There is little argument that the amount of money provided by the Federal government is insufficient to meet all of HAVA's mandates. However, there is an increasing indication that the Federal government will look to the Chief State Election Officials to see to it that their states meet HAVA's mandates and spend the funds in line with Federal and state requirements.

It is also clear that HAVA's authors clearly saw information technology as providing a set of important tools in reforming U.S. elections. Whether talking about voting systems or voter registration systems, the law is replete with discussions of upgrading and reviewing elections technology. While the law's language is circuitous in various places, there are two central technology messages. First, voters in the United States should not be denied access to the ballot because of old voting technology or inappropriate applications of old voting technology. Second, voter registration lists should be current, accurate, and available when needed.

HAVA's drafters also realized that any voting technology carried with it risks of defects, abuse, and fraud. These problems go back to the very beginning of elections. New voting technology is unique only in that it brings **new** risks, not in that it brings any risks. However, the new risks are not necessarily well known. So, HAVA's drafters spent time to assure that the Federal government and the states' election officials would pay due attention to these risks in their implementation of the new technology.

Appendix 1 contains major HAVA sections that address "security" issues associated with voting and voter registration. The issues range from studies to direct mandates to use "technological security measures" to protect the confidentiality, integrity, and availability of statewide voter registration systems.

Confidentiality. Integrity. Availability. Those characteristics virtually define information systems security. The Ohio Secretary of State's Office has taken these matters seriously enough to warrant early steps to assure the security of Ohio's elections infrastructure. Without waiting for the expenditures to be made and the elections to pass, the Secretary has undertaken two straightforward steps to prepare for the security responsibilities that will materialize with development of a statewide voting system and a statewide voter registration system.

Previous Ohio Voting System Vendor Evaluation

The first step was to initiate a very rapid, high-level review of the information system security practices of the main vendors in consideration to provide voting systems to Ohio's counties.

The Secretary acted in 2003 to procure vendors to provide voting systems to Ohio's counties. Through an intensive and exhaustive procurement process, the Secretary's office evaluated vendors' offerings and credentials, narrowing the list to five vendors. In a subsequent phase, the vendor list shrank to four candidates.

In that phase's evaluation, the Secretary took the straightforward step of asking vendors to provide basic information on their information systems structures and practices. The following excerpt from "Vendor Proposal Evaluation Findings Report & Addendum" (Appendix 1, Document ID# O016) summarizes the rationale, conclusions, and recommendations:

> "To help identify and address any risks associated with the information-system security practices and procedures, of the five vendors evaluated in Phases 2 through 4, SOS requested a review by an independent agency. The agency was asked to:
>
> • Review the federal Independent Test Authority (ITA) test results for the five vendors,
>
> • Prepare questions for the vendors to obtain information about their current and planned information-system security practices and procedures, and
>
> • Make recommendations for actions to strengthen the information security practices and procedures of the five vendors.
>
> The survey questions and responses are summarized on the next page. According to "Voting System Vendor Information System Security Review", 08 August 2003, the conclusions and recommendations of the independent evaluation agency's review are:

Conclusions

1. The vendors passed the ITA's tests and requirements regarding security of their hardware, firmware, and software.

2. It is likely that evolving test standards will increase both the emphasis and rigor of security requirements to be met during testing.

3. Some of the vendors do not have a full suite of strong information-system security practices and procedures that might be expected in such a sensitive environment. (However, all expressed a willingness to improve, as shown in the survey responses summarized on the next page.)

Recommendations

1. Require the vendors to demonstrate and document that the hardware, firmware, and software versions they are proposing (and subsequently installing in the election jurisdictions) are those that have been tested and certified.

2. Require the vendors to make a commitment now to meet new Federal standards as the Election Assistance Commission and the National Institutes of Standards and Technology promulgate them.

3. Require the vendors, through their contracts with the State, to provide the Ohio Secretary of State with documentation relating to their firms' information-system security practices and procedures.

Voting Systems

To eliminate and/or reduce identified risks, the evaluation team developed a mitigation plan. The mitigation plan includes an evaluation of voting-system security by an independent agency. At the Secretary of State's request, an independent agency will conduct a security review of the viable vendor(s) voting system(s) to determine whether any security issues exist with the voting system(s), and if so, to recommend the appropriate actions the State should take to address the issues. This review will be conducted after the State's list of viable vendor(s) has been finalized."

Research Methods

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

- Requirements tested
- Test scenarios used
- Test results

- Risks identified
- Likelihood and impact of identified risks
- Risk mitigation strategies
- Recommendations

The scope of this Compuware's effort was to provide a Security Assessment for the DRE voting systems listed in Table 1:

Table 1.
Voting Systems Tested by Compuware

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

The third step undertaken by the Secretary was to carry out the evaluation of Ohio's voting system vendors' security plans, procedures, and processes. It is important to note that this portion of the Security Assessment was not limited just to the four DRE systems proposed in Ohio. It covered all information systems security procedures in the voting system firms. In general terms, this portion of the assessment followed the Ohio Department of Administrative Services' "Information Security Framework" that is in Appendix 2.

This step also included an evaluation of requirements for the Secretary's office to manage and administer election system security statewide. This step called for assessing the information system plans, policies, and procedures that the Secretary's office will need to develop in order to meet the responsibilities placed on the Secretary and to serve the counties as they execute their election responsibilities.

The Secretary of State's Office selected InfoSENTRY Services, Inc. to carry out this assessment and prepare a set of findings and recommendations regarding how the Secretary can go about implementing the best security practices in his office.

InfoSENTRY used a standard approach to the security assessment. The initial step was to request base documentation on information system security practices at the four vendors facilities.

1. Copies of documentation for the vendor's efforts to achieve continued compliance with Federal 2002 voting system standards' configuration management and security requirements.
2. The vendor's information system security plan covering all information systems involved in the design, development, sale, distribution, maintenance, and support of the voting systems.
3. An information system network configuration management plan (if not included in the system security plan) covering all hardware and the network architecture for all information systems involved in the design, development, sale, distribution, maintenance, and support of the voting systems.
4. An information system software configuration management plan (if not included in the system security plan) covering voting devices and information systems involved in their design, development, sales, distribution, maintenance, and support.
5. A copy of the vendor's security policies and procedures covering all information systems involved in the design, development, sale, distribution, maintenance, and support of the voting systems, if those policies and procedures are not contained in and identified clearly in the information system security plan.
6. A copy of any security incident logs maintained for all information systems involved in the design, development, sale, distribution, maintenance, and support of the voting systems.
7. An overall organization chart of the organizations and individuals involved in the design, development, sale, distribution, maintenance, and support of the voting systems that will be offered for use in Ohio's election jurisdictions.
8. An information system security staffing plan including the name(s) of the person or persons who fill the role of information system security officer of chief information security officer with responsibility and accountability for the security of all systems involved in the design, development, sale, distribution, maintenance, and support of the voting systems.
9. Copies of résumés of managers and other technical staff involved in the design, development, sale, distribution, maintenance, and support of the voting systems.
10. Documentation of any systems security-related training courses attended by or systems security-related certifications held by any personnel directly involved in the design, development, sale, distribution, maintenance, and support of the voting systems (if these courses or certifications are not reflected on the résumés requested above).

11. Copies of any security awareness program documentation for any company teams or groups directly involved in the design, development, sale, distribution, maintenance, and support of the voting systems.
12. A copy of the most recent security audit(s) and management response(s) to the audit's findings for all information systems and organizations involved directly in the design, development, sale, distribution, maintenance, and support of the voting systems.
13. A copy of the most recent risk assessment(s) for all business processes and information systems involved directly in the design, development, sale, distribution, maintenance, and support of the voting systems, if the risk assessment material is not contained in and identified clearly in the information system security plan.
14. A copy of the current disaster recovery or business continuity plan for all business processes and information systems involved in the design, development, sale, distribution, maintenance, and support of the voting systems.
15. A copy of the results of the disaster recovery or business continuity plan test(s) for all business processes and information systems involved in the design, development, sale, distribution, maintenance, and support of the voting systems.
16. A copy of the most recent notification of ISO 9000 family of certifications for all organizations and business processes directly involved in the design, development, sale, distribution, maintenance, and support of the voting systems. (It will be helpful to receive also the date of initial certification(s)).
17. A copy of any notification of BS7799 or ISO17799 security certification for all systems involved in the design, development, sale, distribution, maintenance, and support of the voting systems.
18. A copy of technical documentation of (a) current voting system capabilities to provide a voter verifiable paper audit trail and (b) detailed plans for the voting system capabilities to provide a voter verifiable paper audit trail.
19. Copies of user documentation available from the vendor to the Ohio Secretary of State's office or Ohio's counties instructing them on operating and maintaining the voting systems.
20. A copy of the vendors' internal test plan(s) for **(a)** the voting systems proposed to the State of Ohio and **(b)** the voting systems that are currently moving through the certification process according to the 2002 Federal voting system standards (if those systems are not the same).
21. A copy of the test scripts and their results for the voting systems that relate to the security functions and capabilities of the systems in 20(a) and 20(b) above.

Finally, the InfoSENTRY reviewer traveled to offices designated by the vendors meet with senior technical managers and staff members. The vendors selected the following locations for the onsite reviews:

Diebold Election Systems, Vancouver, British Columbia
Election Systems & Software, Omaha, Nebraska
Maximus/Hart InterCivic, Lafayette, Colorado
Sequoia Voting Systems, Denver, Colorado

Prior to arrival, InfoSENTRY sent additional questions and documentation requests. At each site, the InfoSENTRY reviewer met with staff, reviewed documentation, and observed software operations.

Both firms independently prepared their findings and recommendations with very little collaboration or influence on the others' activities.

We note at this point that none of our findings or recommendations can be construed as an endorsement of any of the firm's voting equipment or system capabilities. No implication can be derived from our analysis of the security characteristics of the systems that one system will meet all the election administration requirements of any of Ohio's counties better than will another system.

Summary of Source Code Findings and Recommendations

Table 2 contains a numerical summary of the number of test scenarios in Compuware's code review, platform, and physical tests of the four vendors' systems.

Table 2.
Number of Test Scenarios: By Type and By Vendor

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

Hart InterCivic's system was the subject of one test less than the other systems because an architectural difference in that system's design rendered one test not applicable.

Compuware's report recommends a risk mitigation strategy for each of the risks the firm identified. These vendor specific mitigation strategies for each vendor are in the "Recommended Risk Mitigation Strategy" sections of Compuware's report. The goal of each recommended risk mitigation strategy is to reduce the level of risk to the electronic voting system to an acceptable level.

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

Compuware Recommendation 1: The SOS should implement an Information Technology and Security Policy Standards Document for all related material within any election using a DRE system.

Compuware Recommendation 2: The SOS needs to consider the creation of a Security Director position to oversee Policies, Procedures, Information Technology and Security concerns regarding any election in which a DRE system is used.

Compuware Recommendation 3: The SOS should consider the implementation of a statewide set of security policies and standards for all counties to follow when using any DRE system.

Compuware Recommendation 4: After the above three recommendations have been addressed, the SOS will need to consider the creation of a formal Security Training and Awareness Program for all counties.

Compuware Recommendation 5: The SOS should require Ohio Voting Machine vendors to demonstrate their software development capabilities by achieving Software Engineering Institute CMM Level 2 certification within one year and achieving CMM Level 3 certification within three years.

Compuware Recommendation 6: As new versions of DRE software and hardware are released for use in Ohio, the SOS should conduct independent testing similar to this assessment to ensure the voting systems continue to meet all necessary security requirements.

InfoSENTRY concurs with all of these recommendations. Readers will see in a subsequent section that InfoSENTRY has develop several recommendations that parallel and reinforce these made by Compuware.

Plans, Policies, Procedures: Findings and Recommendations

Volumes 2 through 6 of InfoSENTRY's analysis deal with information systems plans policies and procedures in the following organizations:

- Volume 2: The Ohio Secretary of State's Office
- Volume 3: Diebold Election Systems
- Volume 4: Election Systems and Software
- Volume 5: Hart InterCivic
- Volume 6: Sequoia Voting Systems

In many respects the findings in these volumes point to a very intended consequence of the Secretary of State's Ohio Election Reform strategy: changing the security landscape of elections in Ohio.

There is a principle in physics known commonly as the Heisenburg Uncertainty Principle (HUP). Loosely stated, it holds that the act of measuring or even observing something changes the thing that is being measured or observed. This principle has bedeviled physicist for decades. It means that you introduce possible changes in behavior of something that you are trying to study just by studying it.

However, the Ohio Secretary of State has migrated the Heisenburg Uncertainty Principle from the realm of physics to the realm of election reform and HAVA implementation. By ordering this Security Assessment, the Ohio Secretary of State intended both to observe the condition of security of computerized voting systems and to affect positively and proactively the process of election information system security in Ohio and in the vendors supplying voting systems to Ohio's counties.

Instead of reflecting weakness of measurement, this Security Assessment uses the measurement itself as a means of requiring voting systems vendors and his own office to better equip themselves to handle the security demands of Ohio's election reforms.

As the InfoSENTRY evaluator collected documentation and carried out onsite visits, it was evident that some of the vendors have already started to change their information system security planning processes and procedures very much in line with the questions asked in the Security Assessment in August of this year. Since asking the vendors if they have carried out security risk assessments in August, three vendors have already hired outside firms to carry out just such an assessment. Since asking the vendors if they have business continuity plans, one vendor has developed a plan and schedule a full test for January 2004. Since asking vendors if they are providing advanced security management training for their information systems (IS) staff, one vendor IS director started preparation for the Certified Information Systems Security Professional examination and another has schedule training in implementing the BS7799 security management standard for their company.

InfoSENTRY's research indicates considerable variation in how the vendors follow many of the information systems industry's recommended practices for enhanced system security. None of the vendors meets all of the current recommended practices. None of the vendors falls so far short of standard expectations as to present an unacceptable level of security that cannot be mitigated before the next Federal election in which the equipment will be used.

For each of the vendors, InfoSENTRY has a series of findings and recommendations designed to assist them in moving toward much greater compliance with generally accepted information system security practices. The following section contains those findings and recommendations. In some instances in which there is only a positive finding with no mitigation efforts required, there will be no recommendation associated with the finding.

Findings and Recommendations for the Secretary of State's Office

FINDING OHSOS-01: The Ohio Secretary of State has plans for the imminent deployment of election, voting, and voter registration technology involving advanced information systems and telecommunication that will require significantly greater planning in order to assure the confidentiality, integrity, and availability.

RECOMMENDATION OHSOS-01.1: The Ohio Secretary of State should develop an information system security plan covering all voting and voter registration systems over which the Secretary has authority and for which it has responsibility under HAVA.

RECOMMENDATION OHSOS-01.2: The Secretary of State's Office should conduct an internal, annual risk assessment of voting and voter registration systems throughout Ohio.

RECOMMENDATION OHSOS-01.3: The Secretary of State's Office should have the security plan independently audited at least once in every two-year election Federal election cycle.

RECOMMENDATION OHSOS-01.4: The Secretary of State's Office should develop detailed security policies and procedures covering voting and voter registration systems over which the Secretary has authority and for which it has responsibility under HAVA.

RECOMMENDATION OHSOS-01.5: The Secretary of State's Office should develop a centrally managed, automated system, for use in all 88 of Ohio's counties, for (1) logging, tracking, responding to, and resolving election and voter registration system security incidents and (2) logging, tracking, and analyzing all voting system equipment and software malfunctions and repairs.

FINDING OHSOS-02: The Ohio Secretary of State's Office does not have experienced, certified information technology staff members with the available time and support resources to prepare and administer a statewide voting and voter registration information system security plan.

RECOMMENDATION OHSOS-02.1: The Secretary of State's Office should create the position of Chief Election Systems Security Officer responsible for administering the election system security management plan recommended earlier.

FINDING OHSOS-03: There is no consistent, integrated security awareness and training plan cutting across Ohio's county election officials and vendors.

RECOMMENDATION OHSOS-03.1: The Secretary of State's Office should develop—through careful coordination with county election officials, voting system vendors, and parties involved in implementation of the statewide voter registration system—an integrated, comprehensive information system security awareness and training program.

RECOMMENDATION OHSOS-03.2: The Secretary of State's Office should establish an information security training and certification plan for its information systems staff.

FINDING OHSOS-05: The Ohio Secretary of State's Office has a business continuity plan covering its office and current business requirements that will provide a good foundation for development of a greatly expanded plan covering voting and voter registration information systems.

RECOMMENDATION OHSOS-05.1: The Secretary of State's Office should expand the current business continuity plan's coverage within the next two years to prepare for the full deployment of new voting and voter registration systems prior to January 1, 2006.

Findings and Recommendations for Diebold Election Systems

FINDING Diebold-01: Diebold Election Systems indicates that it has corrected all security-related issues found in the ITA certification process and provides documentation that it is working to achieve necessary ITA certification recommendations for new versions and releases.

FINDING Diebold-02: Diebold Election Systems has a well-defined information systems security organization and an established set of security planning documents.

RECOMMENDATION Diebold-02.1: Diebold Election Systems should review current information systems security management planning documents and align them completely with Ohio's State template as specified in the "Information Security Framework" or as specified in another industry-standard format.

FINDING Diebold-03: Diebold Election Systems has a well-defined set of information systems security policies and clearly defined security procedures.

FINDING Diebold-04: The State of Maryland recently carried out a detailed risk assessment of Diebold Election Systems and the firm has had various other groups assess its overall risk profile.

RECOMMENDATION Diebold-04.1: Diebold should consider having an annual independent, detailed audit by a Certified Information System Auditor of the information system infrastructure and software development operations at Diebold Election Systems.

FINDING Diebold-05: Diebold has experienced, senior information systems security managers available through both Diebold, Inc. and Diebold Election Systems, most of whom have pursued advanced systems security training and certification.

FINDING Diebold-06: Diebold Election Services has basic security awareness procedures in place, but has not elevated overall security awareness and training to a visible stature in the firm.

RECOMMENDATION Diebold-06.1: Diebold Election Systems should develop a formal, on-going security awareness and training program for all of its employees and include additional security awareness materials in its product manuals.

FINDING Diebold-07: Diebold, Inc. has business continuity plans and planning processes, which include agreements with offsite recovery centers and "reciprocal arrangements" with an alternative facility for its primary voting terminal manufacturing site, but it has not tested the plans globally to determine the steps and time required to recover and resume full development or production activities.

RECOMMENDATION Diebold-07.1: Diebold Election Systems should consider carrying out a formal desktop recovery exercise for its software development facilities in Vancouver.

FINDING Diebold-08: Diebold's manufacturing facilities have achieved ISO9000-family process certifications and the software development site has successfully completed an ISO9000-family process certification audit.

RECOMMENDATION Diebold-08.1: In addition to maintaining its certification, Diebold should consider undertaking a commitment to achieve CMMI Level 2 status to improve its overall software maturity capabilities.

FINDING Diebold-09: Diebold is developing a capability to incorporate the ability to prepare a "voter verifiable paper audit trail" if Federal or State of Ohio standards require that functionality.

(There are no standards available for the hardware, firmware, and software that will be required to support this capability. However, Diebold, ES&S, Hart, and Sequoia are committed to provide the capability if it is mandated or demanded by a sufficient portion of the market. The vendors are confident that election jurisdictions can use their current [and future] versions of DRE voting systems to conduct secure elections without the need to produce a voter verifiable paper audit trail.)

Summary of Findings and Recommendations for ES&S

FINDING ES&S-01: ES&S maintains close contact with testing and certification authorities, clearing test exceptions and issues, and moving new versions of products through certification processes.

FINDING ES&S-02: ES&S does not have an information system security management plan that would be consistent with Ohio's IS security management planning standard as outlined in the Information Security Framework.

RECOMMENDATION ES&S-02.1: ES&S should prepare a documented information system security management plan consistent with Ohio's IS security management planning standard or another internationally recognized planning standard.

FINDING ES&S-03: ES&S applies standard configuration management techniques and automated monitoring technologies to its hardware, firmware, and software systems.

FINDING ES&S-04: ES&S maintains numerous information systems security policy and procedures documents, anchored by a recently created information security policies paper.

RECOMMENDATION ES&S-04.1: ES&S should gather its information system security policies and procedures into a single policies and procedures document based on a more generally accepted, industry-standard format for security policies and procedures documentation.

FINDING ES&S-05: ES&S has not performed an internal, detailed security risk assessment on its full information systems infrastructure and products.

RECOMMENDATION ES&S-05.1: ES&S should prepare an internal, detailed security risk assessment based on published industry standards covering all of its information systems infrastructure and products.

FINDING ES&S-06: ES&S has had a minimal security audit, although the audit focused primarily on issues dealing with the firm's financial systems.

RECOMMENDATION ES&S-06.1: ES&S should have a Certified Information System Auditor or an auditor certified to conduct audits under other internationally recognized security auditing standards conduct a detailed security audit on all of the firm's information systems infrastructure and products.

FINDING ES&S-07: The ES&S senior IS administrator and IS staff members have received a wide range of technical training, but have not received recent significant training on the broad discipline of information security.

RECOMMENDATION ES&S-07.1: ES&S should work with its senior IS administrator and other IS staff members to develop for them an IS security training program, with at least one staff member moving toward certification within the next year in IS security or one of its sub-disciplines.

FINDING ES&S-08: ES&S has basic security awareness procedures in place, but has not elevated overall security awareness and training to a visible stature in ES&S.

RECOMMENDATION ES&S-08.1: ES&S should develop a formal, on-going security awareness and training program for all of its employees.

FINDING ES&S-09: ES&S started an outline for a business continuity plan, but has not developed an enterprise-wide plan to cover all critical business functions.

RECOMMENDATION ES&S-09.1: ES&S should prepare, within the next 6-12 months, an enterprise-wide business continuity plan for all critical business functions involved with the design, development, manufacture, sales, and support of the products it has proposed for use in Ohio.

RECOMMENDATION ES&S-09.2: After establishing the business continuity plan, ES&S should carry out a formal desktop recovery exercise for its corporate headquarters and development staff.

FINDING ES&S-10: ES&S's offshore manufacturing facilities in Asia have achieved ISO-9000-family quality process certifications, but the firm's other facilities for software development and customer support have not received such quality certifications.

RECOMMENDATION ES&S-10.1: In addition to obtaining ISO-9000-family certifications for its software development processes and facilities, ES&S should undertake a project to achieve CMMI Level 2 status in order to improve its overall software maturity capabilities.

FINDING ES&S-11: ES&S is developing the ability to prepare a "voter verifiable paper audit trail" if Federal or State of Ohio standards require that functionality.

Summary of Findings and Recommendations for Hart InterCivic

FINDING Hart-01: Hart InterCivic maintains close contact with testing and certification authorities, clearing test exceptions and issues and moving new versions of products through certification process.

FINDING Hart-02: Hart InterCivic has considerable information system planning documentation and well-documented security planning processes, but they are not in a format that is consistent with integrated security planning documentation such as that detailed in Ohio's Information Security Framework or other international security planning documentation standards.

RECOMMENDATION Hart-02.1: Hart InterCivic should pull together its existing security management planning documentation into a format that is established in Ohio's Information Security Framework or another industry-recognized structures for information security management plans.

FINDING Hart-03: Hart InterCivic applies basic configuration management and change control techniques to its application development processes, but needs additional documentation and standardization of those processes.

RECOMMENDATION Hart-03.1: Hart InterCivic should devise and implement very strict, unified configuration management and change control procedures to all of its application development steps and assemble its documentation on those procedures into a cohesive, documented hardware, network, and software configuration management plan within the next 3 – 6 months.

FINDING Hart-04: Hart InterCivic maintains numerous information systems security policy and procedures documents, organized well according to requirements for submittal to ISO auditors and incorporation in an information system security plan.

FINDING Hart-05: Hart InterCivic has hired external consulting firms to prepare detailed network assessment and security risk assessments on its full information systems infrastructure and products.

FINDING Hart-06: Hart InterCivic has had no regular security audit of its critical business functions and information systems infrastructure.

RECOMMENDATION Hart-06.1: Hart InterCivic should have a Certified Information System Auditor or a professional certified as an information security auditor conduct an audit of its IS systems and operations within the next 6 – 12 months.

FINDING Hart-07: Hart InterCivic has provided information security training to its Operations and Information System (IS) Director, with more training scheduled in December.

FINDING Hart-08: Hart InterCivic has an on-going, documented information security awareness program and has provided an online security awareness course to all employees, including senior managers.

FINDING Hart-09: Hart InterCivic has recently developed a business continuity plan, but has tested only portions of that plan.

RECOMMENDATION Hart-09.1: After editing and revising its existing business continuity plan to add some missing details, Hart InterCivic should carry out a formal desktop recovery exercise covering at least its corporate headquarters and development staff.

FINDING Hart-10: Hart InterCivic and its contract-manufacturing partners have achieved ISO-9001 quality process certifications.

RECOMMENDATION Hart-10.1: In addition to its ISO-9000-family certifications for its software development processes and facilities, Hart InterCivic should undertake a project to achieve CMMI Level 2 status in order to improve its overall software maturity capabilities.

FINDING Hart-11: Hart InterCivic is in the planning stages for an ability to prepare a "voter verifiable paper audit trail" if Federal or State of Ohio standards require that functionality.

Summary of Findings and Recommendations for Sequoia Voting Systems

FINDING Sequoia-01: Sequoia maintains close contact with testing and Federal and state certification authorities, clearing test exceptions and issues and moving new versions of products through certification process.

FINDING Sequoia-02: Sequoia has considerable information system planning documentation and well-documented security planning processes as they move to comply with De LaRue security standards. However, the documentation is not in a format that is consistent with integrated security planning documentation such as that detailed in Ohio's Information Security Framework or other international security planning documentation standards.

RECOMMENDATION Sequoia-02.1: Sequoia should adopt the format that is established in Ohio's Information Security Framework or another industry-recognized structure for information security management plans as it moves to meet the parent firm's security guidelines.

FINDING Sequoia-03: Sequoia applies basic configuration management and change control techniques to its application development processes, but needs additional documentation and standardization of those processes.

FINDING Sequoia-04: Sequoia has a well-organized and comprehensive security policy and procedures manual.

FINDING Sequoia-05: Sequoia has not had an external network security assessment nor has it conducted a detailed security risk assessment on its full information systems infrastructure and products.

RECOMMENDATION Sequoia-05: Sequoia Voting Systems should prepare a network security assessment and a detailed security risk assessment on it information systems infrastructure and products.

FINDING Sequoia-06: Sequoia has had a security audit of its critical business functions and information systems infrastructure.

FINDING Sequoia-07: Sequoia senior IS managers have not had recent security-specific training, although the IS Director is planning to take the CISSP examination in December.

RECOMMENDATION Sequoia-07.1: The Sequoia IS Director should continue with certification efforts and examine the possibility of taking courses in BS7799 implementation procedures.

FINDING Sequoia-08: Sequoia has made strides at on-going security awareness measures through frequent e-mail alerts to employees and customers about security incidents and practices.

RECOMMENDATION Sequoia-08.1: Sequoia would benefit from greater planning and formalization of a security awareness program.

FINDING Sequoia-09: Sequoia has a business continuity plan that covers all of its operations, although the Denver office is not considered to be critical to the day-to-day operations of the firm.

FINDING Sequoia-10: Sequoia's contract manufacturing firm has achieved ISO 9001-2000 certification, but Sequoia itself has not sought this certification, indicating that there are no concrete discussions underway about doing so.

RECOMMENDATION Sequoia-10.1: Sequoia should undertake to obtain ISO 9001-2000 certification and move to be certified at CMMI Level 2.

FINDING Sequoia-11: Sequoia is in the prototype development stage for an ability to prepare a "voter verifiable paper audit trail" if Federal or State of Ohio standards require that functionality.

General Findings and Recommendations

An analysis of the detailed work by Compuware and InfoSENTRY reviewers leads to several general findings and recommendations about the condition of computerized voting systems and steps that will lead to their more secure use in Ohio.

InfoSENTRY Finding 1: While significant security issues surround the use of computerized voting systems offered by the four vendors to Ohio, there is no set of risks so great as to warrant a discontinuation of the project to introduce those systems in Ohio's Counties.

Given the relatively early stages of implementation and given that the vendor contracts have not been made final, there is ample time to take steps to mitigate the risks identified in both phases of this Security Assessment.

InfoSENTRY Recommendation 1: Vendors should be required as a condition of its contract with the State to file a detailed, step-by-step plan within 30 days from acceptance of this recommendation by the Secretary of State to mitigate the security risks identified in the Compuware vendor-specific assessments and to improve their security plans, policies, procedures, and processes according to the recommendations in the InfoSENTRY vendor-specific assessments.

Vendors should submit the plans within 30 days, and when the Secretary determines those plans to be acceptable or requires modifications to make them acceptable, Ohio's counties should be allowed to begin purchases of the systems according to rules and guidelines established by the Secretary of State. In order to be acceptable to the Secretary of State, the vendor's risk mitigation plans must specify completion of steps to mitigate all risks identified by InfoSENTRY and Compuware not later than 30 September 2004.

InfoSENTRY Finding 2: A requirement now exists for the Ohio Secretary of State's Office, Ohio's local election officials, and the vendors to focus in concert on programs to improve the secure use of computerized voting systems and mitigate risks associated with that use.

InfoSENTRY Recommendation 2: The Secretary of State, working in close coordination with local election officials, should establish a statewide election information system security incident reporting structure.

Election officials around the state should have a **single point of contact** at the State level to which they should report **any incident** that they believe affects the confidentiality, integrity, of availability of voting systems, regardless of type or manufacturer. Several of the vendors interviewed in this Assessment report use of

internal incident reporting systems. They should be willing and able to assist the State in designing a simple, common-sense, economical way for local election personnel to report election information system security incidents quickly and accurately to the single point of contact in the Secretary of State's Office.

InfoSENTRY Recommendation 3: The Secretary of State should examine the feasibility and cost of creating a statewide voting system defect and repair database.

The State should examine the feasibility of implementing by the November 2006 General Election a statewide database tracking system, used by the vendors, to report all defects and repair operations by machine serial number, firmware version number, software package and version number, date of notification of failure, date of repair, brief nature of the defect, name of the person reporting the defect, and the name of the person responsible for making the repair.

Vendors have varying types of systems by which they track both manufacturing defects and defects that occur when the systems are in use. If nothing else, the Secretary of State's Office can define a common data format that the vendors must use in transmitting **weekly** reports of system defects reported to them from every Ohio county in which they conduct business. Counties should have direct access to the system both to inquire on the database and to enter their own records of defects and repair actions on systems.

This approach would place the onus largely on the vendors to detect, correct, and report system defects, with reports distributed to local election officials for review and verification. Additionally, state staff should be able to generate statistical reports to compare equipment failure rates and determine if any unusual patterns of failure occur.

The Secretary's feasibility study for this kind of system should take no more than three months to complete.

InfoSENTRY Recommendation 4: The Secretary of State's office should establish a formal, documented security awareness and training program for Ohio's election officials.

Both InfoSENTRY and Compuware came to this same conclusion. At the risk of introducing déjà vu all over again, the Secretary of State's office should coordinate efforts among vendors and county election officials to develop vendor-specific security awareness materials and training courses. Some of Ohio's vendors have already started development of security-focused sections in their manuals. Others lag in this area. All should be expected to hit a high level of performance in developing their own security awareness and training programs and expanding that focus out to Ohio's counties.

Conclusion

Systems security is a process, not just a fixed condition of a particular technology. Unlike the assumptions of many critics of computerized election information systems, steps such as simply fixing one vendor's use of encryption, modifying another vendor's failure to control buffer overflows, and correcting another vendor's improper use of multiple execution steps on one line of code will not in and of themselves create secure voting systems. They are important, basic steps in the process of improving voting systems security, but many other steps need to follow.

Ohio's Secretary of State has undertaken an aggressive program to assess voting system security, including the condition of vendor's hardware, software, and data transfers. The Security Assessment points up that no system can be truly secure until the plans, policies, and procedures of all of the voting system supply chain links are made stronger. The Security Assessment found no "show stopper" to indicate that the introduction of computerized voting systems in Ohio should be slowed or stopped **solely because of security concerns.** The Security Assessment found that Ohio's election officials and the vendors who supply them with these systems must take many important mitigating steps in the near future to remedy security problems that do exist.

Appendix 1: Principle HAVA Security Sections

SEC. 221. TECHNICAL GUIDELINES DEVELOPMENT COMMITTEE.

(a) Establishment.--There is hereby established the Technical Guidelines Development Committee (hereafter in this part referred to as the "Development Committee").

(b) Duties.--

(1) In general.--The Development Committee shall assist the Executive Director of the Commission in the development of the voluntary voting system guidelines.

(2) Deadline for initial set of recommendations.--The Development Committee shall provide its first set of recommendations under this section to the Executive Director of the Commission not later than 9 months after all of its members have been appointed.

(c) Membership.--

(1) In general.--The Development Committee shall be composed of the Director of the National Institute of Standards and Technology (who shall serve as its chair), together with a group of 14 other individuals appointed jointly by the Commission and the Director of the National Institute of Standards and Technology, consisting of the following:

(A) An equal number of each of the following:

(i) Members of the Standards Board.

(ii) Members of the Board of Advisors.

(iii) Members of the Architectural and Transportation Barrier Compliance Board under section 502 of the Rehabilitation Act of 1973 (29 U.S.C. 792).

(B) A representative of the American National Standards Institute.

(C) A representative of the Institute of Electrical and Electronics Engineers.

(D) Two representatives of the National Association of State Election Directors selected by such Association who are not members of the Standards Board or Board of Advisors, and who are not of the same political party.

(E) Other individuals with technical and scientific expertise relating to voting systems and voting equipment.

(2) Quorum.--A majority of the members of the Development Committee shall constitute a quorum, except that the Development Committee may not conduct any business prior to the appointment of all of its members.

(d) No Compensation for Service.--Members of the Development Committee shall not receive any compensation for their service, but shall be paid travel expenses, including per diem in lieu of subsistence, at rates authorized for employees of agencies under subchapter I of chapter 57 of title 5, United States Code, while away from their homes or regular places of business in the performance of services for the Development Committee.

(e) Technical Support From National Institute of Standards and Technology.--

(1) In general.--At the request of the Development Committee, the Director of the National Institute of Standards

and Technology shall provide the Development Committee with technical support necessary for the Development Committee to carry out its duties under this subtitle.

(2) Technical support.--The technical support provided under paragraph (1) shall include intramural research and development in areas to support the development of the voluntary voting system guidelines under this part, including--

(A) the security of computers, computer networks, and computer data storage used in voting systems, including the computerized list required under section 303(a);

(B) methods to detect and prevent fraud;

(C) the protection of voter privacy;

(D) the role of human factors in the design and application of voting systems, including assistive technologies for individuals with disabilities (including blindness) and varying levels of literacy; and

(E) remote access voting, including voting through the Internet.

(3) No private sector intellectual property rights in guidelines.--No private sector individual or entity shall obtain any intellectual property rights to any guideline or the contents of any guideline (or any modification to any guideline) adopted by the Commission under this Act.

(f) Publication of Recommendations in Federal Register.--At the time the Commission adopts any voluntary voting system guideline pursuant to section 222, the Development Committee shall cause to have published in the Federal Register the recommendations it provided under this section to the Executive Director of the Commission concerning the guideline adopted.

SEC. 241. PERIODIC STUDIES OF ELECTION ADMINISTRATION ISSUES.

(a) In General.--On such periodic basis as the Commission may determine, the Commission shall conduct and make available to the public studies regarding the election administration issues described in subsection (b), with the goal of promoting methods of voting and administering elections which--

(1) will be the most convenient, accessible, and easy to use for voters, including members of the uniformed services and overseas voters, individuals with disabilities, including the blind and visually impaired, and voters with limited proficiency in the English language;

(2) will yield the most accurate, secure, and expeditious system for voting and tabulating election results;

(3) will be nondiscriminatory and afford each registered and eligible voter an equal opportunity to vote and to have that vote counted; and

(4) will be efficient and cost-effective for use.

(b) Election Administration Issues Described.--For purposes of subsection (a), the election administration issues described in this subsection are as follows:

(1) Methods and mechanisms of election technology and voting systems used in voting and counting votes in elections for Federal office, including the over-vote and under-vote notification capabilities of such technology and systems.

(2) Ballot designs for elections for Federal office.

(3) Methods of voter registration, maintaining secure and accurate lists of registered voters (including the establishment of a centralized, interactive, statewide voter registration list linked to relevant agencies and all polling sites), and ensuring that registered voters appear on the voter registration list at the appropriate polling site.

(4) Methods of conducting provisional voting.

(5) Methods of ensuring the accessibility of voting, registration, polling places, and voting equipment to all voters, including individuals with disabilities (including the blind and visually impaired), Native American or Alaska Native citizens, and voters with limited proficiency in the English language.

(6) Nationwide statistics and methods of identifying, deterring, and **investigating voting fraud** in elections for Federal office.

(7) Identifying, deterring, and investigating methods of voter intimidation.

(8) Methods of recruiting, training, and improving the performance of poll workers.

(9) Methods of educating voters about the process of registering to vote and voting, the operation of voting mechanisms, the location of polling places, and all other aspects of participating in elections.

(10) The feasibility and advisability of conducting elections for Federal office on different days, at different places, and during different hours, including the advisability of establishing a uniform poll closing time and establishing--

(A) a legal public holiday under section 6103 of

title 5, United States Code, as the date on which general elections for Federal office are held;

(B) the Tuesday next after the 1st Monday in November, in every even numbered year, as a legal public holiday under such section;

(C) a date other than the Tuesday next after the 1st Monday in November, in every even numbered year as the date on which general elections for Federal office are held; and

(D) any date described in subparagraph (C) as a legal public holiday under such section.

(11) Federal and State laws governing the eligibility of persons to vote.

(12) Ways that the Federal Government can best assist State and local authorities to improve the administration of elections for Federal office and what levels of funding would be necessary to provide such assistance.

(13)(A) The laws and procedures used by each State that govern--

(i) recounts of ballots cast in elections for Federal office;

(ii) contests of determinations regarding whether votes are counted in such elections; and

(iii) standards that define what will constitute a vote on each type of voting equipment used in the State to conduct elections for Federal office.

(B) The best practices (as identified by the Commission) that are used by States with respect to the recounts and contests described in clause (i).

(C) Whether or not there is a need for more consistency among State recount and contest procedures used with respect to elections for Federal office.

(14) The technical feasibility of providing voting materials in eight or more languages for voters who speak those languages and who have limited English proficiency.

(15) Matters particularly relevant to voting and administering elections in rural and urban areas.

(16) Methods of voter registration for members of the uniformed services and overseas voters, and methods of ensuring that such voters receive timely ballots that will be properly and expeditiously handled and counted.

(17) The best methods for establishing voting system performance benchmarks, expressed as a percentage of residual vote in the Federal contest at the top of the ballot.

(18) Broadcasting practices that may result in the broadcast of false information concerning the location or time of operation of a polling place.

(19) Such other matters as the Commission determines are appropriate.

(c) Reports.--The Commission shall submit to the President and to the Committee on House Administration of the House of Representatives and the Committee on Rules and Administration of the Senate a report on each study conducted under subsection (a) together with such recommendations for administrative and legislative action as the Commission determines is appropriate.

SEC. 242. STUDY, REPORT, AND RECOMMENDATIONS ON BEST PRACTICES FOR FACILITATING MILITARY AND OVERSEAS VOTING.

(a) Study.--

(1) In general.--The Commission, in consultation with the Secretary of Defense, shall conduct a study on the best practices for facilitating voting by absent uniformed services voters (as defined in section 107(1) of the Uniformed and Overseas Citizens Absentee Voting Act) and overseas voters (as defined in section 107(5) of such Act).

(2) Issues considered.--In conducting the study under paragraph (1) the Commission shall consider the following issues:

(A) The rights of residence of uniformed services voters absent due to military orders.

(B) The rights of absent uniformed services voters and overseas voters to register to vote and cast absentee ballots, including the right of such voters to cast a secret ballot.

(C) The rights of absent uniformed services voters and overseas voters to submit absentee ballot applications early during an election year.

(D) The appropriate preelection deadline for mailing absentee ballots to absent uniformed services voters and overseas voters.

(E) The appropriate minimum period between the mailing of absentee ballots to absent uniformed services voters and overseas voters and the deadline for receipt of such ballots.

(F) The timely transmission of balloting materials to absent uniformed services voters and overseas voters.

(G) Security and privacy concerns in the transmission, receipt, and processing of ballots from absent uniformed services voters and overseas voters, including the need to protect against fraud.

(H) The use of a single application by absent uniformed services voters and overseas voters for absentee ballots for all Federal elections occurring during a year.

(I) The use of a single application for voter registration and absentee ballots by absent uniformed services voters and overseas voters.

(J) The use of facsimile machines and electronic means of transmission of absentee ballot applications and absentee ballots to absent uniformed services voters and overseas voters.

(K) Other issues related to the rights of absent uniformed services voters and overseas voters to participate in elections.

(b) Report and Recommendations.--Not later than the date that is 18 months after the date of the enactment of this Act, the Commission shall submit to the President and Congress a report on the study conducted under subsection (a)(1) together with recommendations identifying the best practices used with respect to the issues considered under subsection (a)(2).

SEC. 245. STUDY AND REPORT ON ELECTRONIC VOTING AND THE ELECTORAL PROCESS.

(a) Study.--

(1) In general.--**The Commission shall conduct a thorough study of issues and challenges, specifically to include the potential for election fraud, presented by incorporating communications and Internet technologies in the Federal, State, and local electoral process.**

(2) Issues to be studied.--The Commission may include in the study conducted under paragraph (1) an examination of--

(A) the appropriate security measures required and minimum standards for certification of systems or technologies in order to minimize the potential for fraud in voting or in the registration of qualified citizens to register and vote;

(B) the possible methods, such as Internet or other communications technologies, that may be utilized in the electoral process, including the use of those technologies to register voters and enable citizens to vote online, and recommendations concerning statutes and rules to be adopted in order to implement an online or Internet system in the electoral process;

(C) the impact that new communications or Internet technology systems for use in the electoral process could have on voter participation rates, voter education, public accessibility, potential external influences during the elections process, voter privacy and anonymity, and other issues related to the conduct and administration of elections;

(D) whether other aspects of the electoral process, such as public availability of candidate information and citizen communication with candidates, could benefit from the increased use of online or Internet technologies;

(E) the requirements for authorization of collection, storage, and processing of electronically generated and transmitted digital messages to permit any eligible person to register to vote or vote in an election, including applying for and casting an absentee ballot;

(F) the implementation cost of an online or Internet voting or voter registration system and the costs of elections after implementation (including a comparison of total cost savings for the administration of the electoral process by using Internet technologies or systems);

(G) identification of current and foreseeable online and Internet technologies for use in the registration of voters, for voting, or for the purpose of reducing election fraud, currently available or in use by election authorities;

(H) the means by which to ensure and achieve equity of access to online or Internet voting or voter registration systems and address the fairness of such systems to all citizens; and

(I) the impact of technology on the speed,

timeliness, and accuracy of vote counts in Federal, State, and local elections.

(b) Report.--

(1) Submission.--Not later than 20 months after the date of the enactment of this Act, the Commission shall transmit to the Committee on House Administration of the House of Representatives and the Committee on Rules and Administration of the Senate a report on the results of the study conducted under subsection (a), including such legislative recommendations or model State laws as are required to address the findings of the Commission.

(2) Internet posting.--In addition to the dissemination requirements under chapter 19 of title 44, United States Code, the Election Administration Commission shall post the report transmitted under paragraph (1) on an Internet website.

SEC. 271. GRANTS FOR RESEARCH ON VOTING TECHNOLOGY IMPROVEMENTS.

(a) In General.--**The Commission shall make grants to assist entities in carrying out research and development to improve the quality, reliability, accuracy, accessibility, affordability, and security of voting equipment, election systems, and voting technology.**

(b) Eligibility.--An entity is eligible to receive a grant under this part if it submits to the Commission (at such time and in such form as the Commission may require) an application containing--

(1) certifications that the research and development funded with the grant will take into account the need to make voting equipment fully accessible for individuals with disabilities, including the blind and visually impaired, the need to ensure that such individuals can vote independently and with privacy, and the need to provide alternative language accessibility for individuals with limited proficiency in the English language (consistent with the requirements of the Voting Rights Act of 1965); and

(2) such other information and certifications as the Commission may require.

(c) Applicability of Regulations Governing Patent Rights in Inventions Made With Federal Assistance.--Any invention made by the recipient of a grant under this part using funds provided under this part shall be subject to chapter 18 of title 35, United States Code (relating to patent rights in inventions made with Federal assistance).

(d) Recommendation of Topics for Research.--

(1) In general.--The Director of the National Institute of Standards and Technology (hereafter in this section referred to as the "Director") shall submit to the Commission an annual list of the Director's suggestions for issues which may be the subject of research funded with grants awarded under this part during the year.

(2) Review of grant applications received by commission.--The Commission shall submit each application it receives for a grant under this part to the Director, who shall review the application and provide the Commission with such comments as the Director considers appropriate.

(3) Monitoring and adjustment of grant activities at request of commission.--After the Commission has awarded a grant under this part, the Commission may request that the Director monitor the grant, and (to the extent permitted under the terms of the grant as awarded) the Director may recommend to the Commission that the recipient of the grant modify and adjust the activities carried out under the grant.

(4) Evaluation of grants at request of commission.--

(A) In general.--In the case of a grant for which the Commission submits the application to the Director under paragraph (2) or requests that the Director monitor the grant under paragraph (3), the Director shall prepare and submit to the Commission an evaluation of the grant and the activities carried out under the grant.

(B) Inclusion in reports.--The Commission shall include the evaluations submitted under subparagraph (A) for a year in the report submitted for the year under section 207.

(e) Provision of Information on Projects.--The Commission may provide to the Technical Guidelines Development Committee under part 3 of subtitle A such information regarding the activities funded under this part as the Commission deems necessary to assist the Committee in carrying out its duties.

SEC. 302. PROVISIONAL VOTING AND VOTING INFORMATION REQUIREMENTS.

(a) Provisional Voting Requirements.--If an individual declares that such individual is a registered voter in the jurisdiction in which the individual desires to vote and that the individual is eligible to vote in an election for Federal office, but the name of the individual does not appear on the official list of eligible voters for the polling place or an election official asserts that the individual is not eligible to vote, such individual shall be permitted to cast a provisional ballot as follows:

(1) An election official at the polling place shall notify the individual that the individual may cast a provisional ballot in that election.

(2) The individual shall be permitted to cast a provisional ballot at that polling place upon the execution of a written affirmation by the individual before an election official at the polling place stating that the individual is--

(A) a registered voter in the jurisdiction in which the individual desires to vote; and

(B) eligible to vote in that election.

(3) An election official at the polling place shall transmit the ballot cast by the individual or the voter information contained in the written affirmation executed by the individual under paragraph (2) to an appropriate State or local election official for prompt verification under paragraph (4).

(4) If the appropriate State or local election official to whom the ballot or voter information is transmitted under paragraph (3) determines that the individual is eligible under State law to vote, the individual's provisional ballot shall be counted as a vote in that election in accordance with State law.

(5)(A) At the time that an individual casts a provisional ballot, the appropriate State or local election official shall give the individual written information that states that any individual who casts a provisional ballot will be able to ascertain under the system established under subparagraph (B) whether the vote was counted, and, if the vote was not counted, the reason that the vote was not counted.

(B) The appropriate State or local election official shall establish a free access system (such as a toll-free telephone number or an Internet website) that any individual who casts a provisional ballot may access to discover whether the vote of that individual was counted, and, if the vote was not counted, the reason that the vote was not counted.

States described in section 4(b) of the National Voter Registration Act of 1993 (42 U.S.C. 1973gg-2(b)) may meet the requirements of this subsection using voter registration procedures established under applicable State law. **The appropriate State or local official shall establish and maintain reasonable procedures necessary to protect the security, confidentiality, and integrity of personal information collected, stored, or otherwise used by the free access system established under paragraph (5)(B). Access to information about an individual provisional ballot shall be restricted to the individual who cast the ballot.**

(b) Voting Information Requirements.--

(1) Public posting on election day.--The appropriate State or local election official shall cause voting information to be

publicly posted at each polling place on the day of each election for Federal office.

(2) Voting information defined.--In this section, the term "voting information" means--

(A) a sample version of the ballot that will be used for that election;

(B) information regarding the date of the election and the hours during which polling places will be open;

(C) instructions on how to vote, including how to cast a vote and how to cast a provisional ballot;

(D) instructions for mail-in registrants and first-time voters under section 303(b);

(E) general information on voting rights under applicable Federal and State laws, including information on the right of an individual to cast a provisional ballot and instructions on how to contact the appropriate officials if these rights are alleged to have been violated; and

(F) general information on Federal and State laws regarding prohibitions on acts of fraud and misrepresentation.

(c) Voters Who Vote After the Polls Close.--Any individual who votes in an election for Federal office as a result of a Federal or State court order or any other order extending the time established for closing the polls by a State law in effect 10 days before the date of that election may only vote in that election by casting a provisional ballot under subsection (a). Any such ballot cast under the preceding sentence shall be separated and held apart from other provisional ballots cast by those not affected by the order.

(d) Effective Date for Provisional Voting and Voting Information.--Each State and jurisdiction shall be required to comply with the requirements of this section on and after January 1, 2004.

SEC. 303. COMPUTERIZED STATEWIDE VOTER REGISTRATION LIST REQUIREMENTS AND REQUIREMENTS FOR VOTERS WHO REGISTER BY MAIL.

(a) Computerized Statewide Voter Registration List Requirements.--

(1) Implementation.--

(A) In general.--Except as provided in subparagraph (B), each State, acting through the chief State election official, shall implement, in a uniform and nondiscriminatory manner, a single, uniform, official, centralized, interactive computerized statewide voter registration list defined, maintained, and administered at the State level that contains the name and registration information of every legally registered voter in the State and assigns a unique identifier to each legally registered voter in the State (in this subsection referred to as the "computerized list"), and includes the following:

(i) The computerized list shall serve as the single system for storing and managing the official list of registered voters throughout the State.

(ii) The computerized list contains the name and registration information of every legally registered voter in the State.

(iii) Under the computerized list, a unique identifier is assigned to each legally registered voter in the State.

(iv) The computerized list shall be coordinated with other agency databases within the State.

(v) Any election official in the State, including any local election official, may obtain immediate electronic access to the information contained in the computerized list.

(vi) All voter registration information obtained by any local election official in the State shall be electronically entered into the computerized list on an expedited basis at the time the information is provided to the local official.

(vii) The chief State election official shall provide such support as may be required so that local election officials are able to enter information as described in clause (vi).

(viii) The computerized list shall serve as the official voter registration list for the conduct of all elections for Federal office in the State.

(B) Exception.--The requirement under subparagraph (A) shall not apply to a State in which, under a State law in effect continuously on and after the date of the enactment of this Act, there is no voter registration requirement for individuals in the State with respect to

elections for Federal office.

(2) Computerized list maintenance.--

(A) In general.--The appropriate State or local election official shall perform list maintenance with respect to the computerized list on a regular basis as follows:

(i) If an individual is to be removed from the computerized list, such individual shall be removed in accordance with the provisions of the National Voter Registration Act of 1993 (42 U.S.C. 1973gg et seq.), including subsections (a)(4), (c)(2), (d), and (e) of section 8 of such Act (42 U.S.C. 1973gg-6).

(ii) For purposes of removing names of ineligible voters from the official list of eligible voters--

(I) under section 8(a)(3)(B) of such Act (42 U.S.C. 1973gg-6(a)(3)(B)), the State shall coordinate the computerized list with State agency records on felony status; and

(II) by reason of the death of the registrant under section 8(a)(4)(A) of such Act (42 U.S.C. 1973gg-6(a)(4)(A)), the State shall coordinate the computerized list with State agency records on death.

(iii) Notwithstanding the preceding provisions of this subparagraph, if a State is described in section 4(b) of the National Voter Registration Act of 1993 (42 U.S.C. 1973gg-2(b)), that State shall remove the names of ineligible voters from the computerized list in accordance with State law.

(B) Conduct.--The list maintenance performed under subparagraph (A) shall be conducted in a manner that ensures that--

(i) the name of each registered voter appears in the computerized list;

(ii) only voters who are not registered or who are not eligible to vote are removed from the computerized list; and

(iii) duplicate names are eliminated from the computerized list.

(3) Technological security of computerized list.--The appropriate State or local official shall provide adequate technological security measures to prevent the unauthorized access to the computerized list established under this section.

(4) Minimum standard for accuracy of state voter registration records.--The State election system shall include provisions to ensure that voter registration records in the State are accurate and are updated regularly, including the following:

(A) A system of file maintenance that makes a reasonable effort to remove registrants who are ineligible to vote from the official list of eligible voters. Under such system, consistent with the National

Voter Registration Act of 1993 (42 U.S.C. 1973gg et seq.), registrants who have not responded to a notice and who have not voted in 2 consecutive general elections for Federal office shall be removed from the official list of eligible voters, except that no registrant may be removed solely by reason of a failure to vote.

(B) Safeguards to ensure that eligible voters are not removed in error from the official list of eligible voters.

(5) Verification of voter registration information.--

(A) Requiring provision of certain information by applicants.--

(i) In general.--Except as provided in clause (ii), notwithstanding any other provision of law, an application for voter registration for an election for Federal office may not be accepted or processed by a State unless the application includes--

(I) in the case of an applicant who has been issued a current and valid driver's license, the applicant's driver's license number; or

(II) in the case of any other applicant (other than an applicant to whom clause (ii) applies), the last 4 digits of the applicant's social security number.

(ii) Special rule for applicants without driver's license or social security number.--If an applicant for voter registration for an election for Federal office has not been issued a current and valid driver's license or a social security number, the State shall assign the applicant a number which will serve to identify the applicant for voter registration purposes. To the extent that the State has a computerized list in effect under this subsection and the list assigns unique identifying numbers to registrants, the number assigned under this clause shall be the unique identifying number assigned under the list.

(iii) Determination of validity of numbers provided.--The State shall determine whether the information provided by an individual is sufficient to meet the requirements of this subparagraph, in accordance with State law.

(B) Requirements for state officials.--

(i) Sharing information in databases.--The chief State election official and the official responsible for the State motor vehicle authority of a State shall enter into an agreement to match information in the database of the statewide voter registration system with information in the database of the motor vehicle authority to the extent required to enable each such official to verify the accuracy of the information provided on applications for voter

registration.

(ii) Agreements with commissioner of social security.--The official responsible for the State motor vehicle authority shall enter into an agreement with the Commissioner of Social Security under section 205(r)(8) of the Social Security Act (as added by subparagraph (C)).

(C) Access to federal information.--Section 205(r) of the Social Security Act (42 U.S.C. 405(r)) is amended by adding at the end the following new paragraph:

"(8)(A) The Commissioner of Social Security shall, upon the request of the official responsible for a State driver's license agency pursuant to the Help America Vote Act of 2002--

"(i) enter into an agreement with such official for the purpose of verifying applicable information, so long as the requirements of subparagraphs (A) and (B) of paragraph (3) are met; and

"(ii) include in such agreement safeguards to assure the maintenance of the confidentiality of any applicable information disclosed and procedures to permit such agency to use the applicable information for the purpose of maintaining its records.

"(B) Information provided pursuant to an agreement under this paragraph shall be provided at such time, in such place, and in such manner as the Commissioner determines appropriate.

"(C) <<NOTE: Procedures.>> The Commissioner shall develop methods to verify the accuracy of information provided by the agency with respect to applications for voter registration, for whom the last 4 digits of a social security number are provided instead of a driver's license number.

"(D) For purposes of this paragraph--

"(i) the term `applicable information' means information regarding whether--

"(I) the name (including the first name and any family forename or surname), the date of birth (including the month, day, and year), and social security number of an individual provided to the Commissioner match the information contained in the Commissioner's records, and

"(II) such individual is shown on the records of the Commissioner as being deceased; and

"(ii) the term `State driver's license agency' means the State agency which issues driver's licenses to individuals within the State and maintains records relating to such licensure.

"(E) Nothing in this paragraph may be construed to require the provision of applicable information with regard to a request for a record of an individual if the Commissioner determines there are exceptional circumstances warranting an exception (such as safety of the individual or interference with an investigation).

"(F) Applicable information provided by the Commission pursuant to an agreement under this paragraph or by an individual to any agency that

has entered into an agreement under this paragraph shall be considered as strictly confidential and shall be used only for the purposes described in this paragraph and for carrying out an agreement under this paragraph. Any officer or employee or former officer or employee of a State, or any officer or employee or former officer or employee of a contractor of a State who, without the written authority of the Commissioner, publishes or communicates any applicable information in such individual's possession by reason of such employment or position as such an officer, shall be guilty of a felony and upon conviction thereof shall be fined or imprisoned, or both, as described in section 208.".

(D) Special rule for certain states.--In the case of a State which is permitted to use social security numbers, and provides for the use of social security numbers, on applications for voter registration, in accordance with section 7 of the Privacy Act of 1974 (5 U.S.C. 552a note), the provisions of this paragraph shall be optional.

(b) Requirements for Voters Who Register by Mail.--

(1) In general.--Notwithstanding section 6(c) of the National Voter Registration Act of 1993 (42 U.S.C. 1973gg-4(c)) and subject to paragraph (3), a State shall, in a uniform and nondiscriminatory manner, require an individual to meet the requirements of paragraph (2) if--

(A) the individual registered to vote in a jurisdiction by mail; and

(B)(i) the individual has not previously voted in an election for Federal office in the State; or

(ii) the individual has not previously voted in such an election in the jurisdiction and the jurisdiction is located in a State that does not have a computerized list that complies with the requirements of subsection (a).

(2) Requirements.--

(A) In general.--An individual meets the requirements of this paragraph if the individual--

(i) in the case of an individual who votes in person--

(I) presents to the appropriate State or local election official a current and valid photo identification; or

(II) presents to the appropriate State or local election official a copy of a current utility bill, bank statement, government check, paycheck, or other government document that shows the name and address of the voter; or

(ii) in the case of an individual who votes by mail, submits with the ballot--

(I) a copy of a current and valid photo identification; or

(II) a copy of a current utility bill, bank statement, government check, paycheck, or other government document

that shows the name and address of the voter.

(B) Fail-safe voting.--

(i) In person.--An individual who desires to vote in person, but who does not meet the requirements of subparagraph (A)(i), may cast a provisional ballot under section 302(a).

(ii) By mail.--An individual who desires to vote by mail but who does not meet the requirements of subparagraph (A)(ii) may cast such a ballot by mail and the ballot shall be counted as a provisional ballot in accordance with section 302(a).

(3) Inapplicability.--Paragraph (1) shall not apply in the case of a person--

(A) who registers to vote by mail under section 6 of the National Voter Registration Act of 1993 (42 U.S.C. 1973gg-4) and submits as part of such registration either--

(i) a copy of a current and valid photo identification; or

(ii) a copy of a current utility bill, bank statement, government check, paycheck, or government document that shows the name and address of the voter;

(B)(i) who registers to vote by mail under section 6 of the National Voter Registration Act of 1993 (42 U.S.C. 1973gg-4) and submits with such registration either--

(I) a driver's license number; or

(II) at least the last 4 digits of the individual's social security number; and

(ii) with respect to whom a State or local election official matches the information submitted under clause (i) with an existing State identification record bearing the same number, name and date of birth as provided in such registration; or

(C) who is--

(i) entitled to vote by absentee ballot under the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff-1 et seq.);

(ii) provided the right to vote otherwise than in person under section 3(b)(2)(B)(ii) of the Voting Accessibility for the Elderly and Handicapped Act (42 U.S.C. 1973ee-1(b)(2)(B)(ii)); or

(iii) entitled to vote otherwise than in person under any other Federal law.

(4) Contents of mail-in registration form.--

(A) In general.--The mail voter registration form developed under section 6 of the National Voter Registration Act of 1993 (42 U.S.C. 1973gg-4) shall include the following:

(i) The question "Are you a citizen of the United States of America?" and boxes for the applicant to check to indicate whether the applicant is or is not a citizen of the United

States.

(ii) The question "Will you be 18 years of age on or before election day?" and boxes for the applicant to check to indicate whether or not the applicant will be 18 years of age or older on election day.

(iii) The statement "If you checked 'no' in response to either of these questions, do not complete this form.".

(iv) A statement informing the individual that if the form is submitted by mail and the individual is registering for the first time, the appropriate information required under this section must be submitted with the mail-in registration form in order to avoid the additional identification requirements upon voting for the first time.

(B) Incomplete forms.--If an applicant for voter registration fails to answer the question included on the mail voter registration form pursuant to subparagraph (A)(i), the registrar shall notify the applicant of the failure and provide the applicant with an opportunity to complete the form in a timely manner to allow for the completion of the registration form prior to the next election for Federal office (subject to State law).

(5) Construction.--Nothing in this subsection shall be construed to require a State that was not required to comply with a provision of the National Voter Registration Act of 1993 (42 U.S.C. 1973gg et seq.) before the date of the enactment of this Act to comply with such a provision after such date.

(c) Permitted Use of Last 4 Digits of Social Security Numbers.--The last 4 digits of a social security number described in subsections (a)(5)(A)(i)(II) and (b)(3)(B)(i)(II) shall not be considered to be a social security number for purposes of section 7 of the Privacy Act of 1974 (5 U.S.C. 552a note).

(d) Effective Date.--

(1) Computerized statewide voter registration list requirements.--

(A) In general.--Except as provided in subparagraph (B), each State and jurisdiction shall be required to comply with the requirements of subsection (a) on and after January 1, 2004.

(B) Waiver.--If a State or jurisdiction certifies to the Commission not later than January 1, 2004, that the State or jurisdiction will not meet the deadline described in subparagraph (A) for good cause and includes in the certification the reasons for the failure to meet such deadline, subparagraph (A) shall apply to the State or jurisdiction as if the reference in such subparagraph to "January 1, 2004" were a reference to "January 1, 2006".

(2) Requirement for voters who register by mail.--

(A) In general.--Each State and jurisdiction shall be required to comply with the requirements of subsection (b) on and after January 1, 2004, and shall

be prepared to receive registration materials submitted by individuals described in subparagraph (B) on and after the date described in such subparagraph.

(B) Applicability with respect to individuals.--The provisions of subsection (b) shall apply to any individual who registers to vote on or after January 1, 2003.

Appendix 2: The State of Ohio's "Information Security Framework"