State of Maryland

Diebold AccuVote-TS

Voting System Security Action Plan

Linda H. Lamone, Administrator
Maryland State Board of Elections
151 West Street, Suite 200
Annapolis, MD 21401

September 23, 2003

Revised: October 24, 2003
November 26, 2003
January 20, 2004
February 6, 2004
February 23, 2004
March 17, 2004
April 7, 2004
July 7, 2004

BACKGROUND

Maryland Election Law Article, Statement of Purpose, intends that the conduct of elections should ensure that:

- All persons served by the election system are treated fairly and equitably;
- All qualified persons may register and vote and that those who are not qualified to vote do not;
- Those that administer elections are well-trained, that they serve both those who vote and those who seek votes, and that they put the public interest ahead of partisan interests;
- Citizen convenience is emphasized in all aspect[s] of the election process;
- Security and integrity are maintained in the casting of ballots, canvassing of votes, and reporting of election results; and
- The prevention of fraud and corruption is diligently pursued.

One of the critical public services of the State Board of Elections' (SBE) is the selection and delivery of a voting system meeting the requirements of law and regulation. Chapter 564 of the Laws of Maryland (2001) requires the selection and certification of a uniform statewide voting system for polling place voting and a uniform statewide voting system for absentee voting. By 2006, all jurisdictions in Maryland are required to use the uniform voting system. Four counties implemented the uniform voting system for the 2002 elections, and nineteen jurisdictions are scheduled to implement the uniform system for the 2004 elections. The remaining jurisdiction, Baltimore City, will implement the system for the 2006 elections.

The Help America Vote Act of 2002 (HAVA) requires that each state have a voting system that complies with the federal requirements outlined in HAVA, as well as a Direct Recording Electronic (DRE) or other accessible voting unit in each precinct for voters with disabilities. Since Maryland's statewide voting system meets the federal requirements and has accessories that allow voters with disabilities to vote secretly and independently, this system complies with the federal voting system accessibility requirement. Once all jurisdictions have implemented the statewide voting system, Maryland will have satisfied this federal requirement.

Through a detailed evaluation of vendor proposals, SBE chose the Diebold Election Systems, Inc. (DESI) AccuVote-Touch Screen (TS) for polling place voting and the Diebold AccuVote Optical Scan for absentee voting. DESI is a wholly owned subsidiary of Diebold, Inc. The agency entered into a contract for the Phase I voting system implementation covering four counties on December 12, 2001. SBE signed a modification to the contract with DESI on July 19, 2003 for up to $55.6 million. The modification included the delivery of voting equipment (AccuVote-Touch Screen and

AccuVote Optical Scan) and services for 19 jurisdictions; a.k.a., Phase II Voting System Implementation.

In a report dated July 23, 2003, entitled "Analysis of an Electronic Voting System," (the Rubin report) computer scientists from Johns Hopkins University and Rice University stated results of their analysis of source code for a DESI voting system. The report addressed security issues and vulnerabilities of DESI source code that was found on a DESI web site. The report acknowledged that the human processes surrounding the source code were not analyzed. Assumptions were made in the Rubin report that are incorrect; e.g., that the system operates on the Internet, which it does not. In addition, SBE and Diebold media outreach efforts pointed out that the State's procedural controls and general voting environment reduce or eliminate many of the vulnerabilities identified in the report. However, these facts were not widely circulated by the media.

The Phase I Voting System Implementation and the lessons learned process employed by the State, SBE, Local Boards of Elections (LBEs) and Diebold identified several issues that needed to be resolved. One of the more significant items was the need to eliminate the "hard-coded" passwords used in the system. As a result of these efforts, Diebold made changes to its software and submitted the revised software to the Independent Testing Authority (ITA) for certification, as required under the Election Assistance Commission (formerly Federal Election Commission) standards for voting equipment.

On August 5, 2003, Governor Robert L. Ehrlich, Jr., directed that an independent review of the security of the Diebold AccuVote-TS Voting System and the election processes surrounding it be performed. The Department of Budget and Management (DBM) and the SBE jointly managed the project. Science Applications International Corporation (SAIC), an independent IT firm with an international reputation and strength in IT security, performed the analysis. In response to the Risk Assessment Report of the Diebold AccuVote-TS Voting System and Processes, this Action Plan was developed.

The Risk Assessment Report reviewed compliance with a total of 328 requirements for voting system security, including management, operational and technical controls.

- Management controls address core or fundamental principles that are inherent in the protection of information systems to manage risk.
- Operational controls focus on protection mechanisms that are primarily planned, implemented and monitored by people.
- Technical controls are generally system or electronically-based and rely heavily on operational and management controls in addition to system-based restrictions.

The risk assessment included testing of a complete AccuVote-TS system, and reviews of administrative procedures and controls for election processing security. A total of

218 requirements were found to be met with existing procedures and technical features. Forty-four requirements were deemed not applicable to this specific system. Sixty-six requirements were found to need further action. Security improvements were found to be needed in each category of requirements; that is, management, operational and technical. These include the following types of actions:

- SBE needs to aggregate existing security policies and procedures into a formal Information System Security Plan (ISSP);
- SBE needs to develop a formal Information System Security Training Program;
- SBE needs to develop a plan for all local jurisdictions to implement policies and procedures uniformly;
- SBE needs to verify that no voting system server is included in an open computer system.

Requirements Table

Number	Requirements Met	Not Applicable	Action Items
328	218	44	66

This Requirements Table segregates requirements SAIC reviewed into categories based on whether the requirement was met or did not apply. Of the 328 requirements evaluated, 80% were judged to already have been met or are not applicable. The remaining 66 were identified as action items. Because many of the items overlap, the 66 items have been condensed into 23 tasks (see Tasks and Schedule section).

Risk Categories Table

Action Items	High	Medium	Low
66	26	16	24

The 66 action items were further segregated into high, medium, and low risk categories. Because many of the items overlap, the 66 items have been condensed into 23 tasks (see Tasks and Schedule section).

It is the opinion of the State Board of Elections that:

1. Management and operational requirements can and will be met so as to fully assure the integrity of the voting process for all voters, including those with disabilities.

2. The Diebold AccuVote-TS system selected by the Board is fully and readily capable of meeting the security requirements with minor modifications, and with appropriate administrative and operational controls.

This Action Plan outlines an overall strategy, tasks and schedule, to fully meet the security requirements of the election process with the Diebold AccuVote-TS equipment, and identifies the resources necessary to implement the Action Plan.

OVERALL DIRECTION

The State Board of Elections recognizes the importance of the role security plays in ensuring secure elections. SBE takes the Risk Assessment Report of the Diebold AccuVote-TS Voting System and Processes seriously and is committed to implementing the report recommendations and taking action to meet the highest standards for the integrity of the voting process.

The Risk Assessment Report revealed certain administrative and procedural changes that are necessary to ensure an overall secure implementation. The administrative and procedural changes will be completed in phases: Phase I by October 13, 2003 (the scheduled start date for User Acceptance Testing of the Diebold Voting System units); Phase II by January 31, 2004 (prior to loading the ballots for the Presidential Primary Election); and Phase III by March 31, 2004 (for the rest of the SBE information systems).

The Department of Budget and Management (DBM) Office of Information Technology (OIT) Information Technology (IT) Security Policy and Standards (Version 1.1 dated July 2003) requires each State agency to develop a security plan for protecting technology systems, including such common technologies as computers, data and voice networks, and other specialized resources. The security plan is necessary because SBE uses information technology to help carry out its public services, one of which is the voting system.

SBE has established comprehensive procedures and processes for the local boards of elections to follow. In addition, at the State level there are extensive procedures and processes that address numerous security issues. The Risk Assessment Report observed, “The State of Maryland procedural controls and general voting environment reduce or eliminate many of the vulnerabilities identified in the Rubin report.” In recognition of the changes in the voting technologies associated with the Diebold AccuVote-TS voting system, SBE intends to reexamine all the existing security procedures and processes and add appropriate additional measures to further safeguard the election process.

SBE will also aggregate the existing procedures and develop and implement a formal Information System Security Plan (ISSP). The ISSP will be based on a framework according to the National Institute of Standards and Technology (NIST) *Guide for*

Developing Security Plans for Information Technology Systems, SP 800-18 (www.csrc.nist.gov), and will include the DBM OIT IT Security Policy and Standards.

The ISSP will be developed in three phases over a period of six months (by March 31, 2004) that will address all the information technologies used by the State Board of Elections. The process of developing and implementing this plan must include involvement of all affected organizations, especially the local boards of elections (LBEs). It is important to obtain their expertise and knowledge of the election process since the LBEs actually conduct the election. The LBEs must ensure the full implementation of and compliance with the formal security plan.

The ISSP will be maintained through a review process when changes are made to the information system and/or processes surrounding it, but no longer than three years between reviews. The State of Maryland Office of Information Technology Risk Assessment of the Diebold AccuVote-TS Voting System and Processes by SAIC in September 2003 establishes the baseline.

The formal Information System Security Training Program will be developed to provide security awareness training to all election officials and contractor personnel in support of the election process. This includes the following:

- State Board of Elections members: 5
- State Administrator and staff: 30
- Local Boards of Elections members: 122
- Local Election Directors and staff (permanent and temporary): 160-200
- Election judges: 18,000 are used for each election
- Contractor personnel: approximately 200 (including special Election Day support personnel).

Therefore, approximately 18,500 people will require training.

RESOURCES

The development of the ISSP and associated implementation plans is expected to cover a relatively short period of time. The necessary resources to develop these can best come from a vendor with expertise and experience in this specialized field. The resources would come from a contractor under an existing State of Maryland contract.

SBE will need three additional personnel to guide the development and implementation of the ISSP. The Risk Assessment Report recommended establishing an SBE Chief Information System Security Officer position. Two additional State contractual positions are needed, one to develop written procedures and facilitate coordination between SBE and the LBEs and one to manage the voter outreach and security training programs.

SBE has received federal funds under the Help America Vote Act of 2002 (HAVA) to implement election reform. The Assistant Attorney General for SBE has provided a legal opinion that developing and implementing the ISSP is an acceptable use of the federal HAVA funds.

TASKS AND SCHEDULE

Phase I

1. Remove SBE Global Election Management System (GEMS) server from SBE local network connections **Completed**

2. Reinstall software on SBE GEMS server **Completed**
   To validate that the system has not been compromised

3. Discontinue use of File Transfer Protocol (FTP) for ballot distribution **Completed**

   NOTE for tasks 1, 2 & 3: The SBE GEMS server was connected to the SBE office LAN (local area network) during the election cycle in 2002. The SBE GEMS server was used only to receive and proof ballots and not to develop the ballots. Additionally, the SBE GEMS server was not used to collect vote totals on election night or after the vote canvass. SBE also used the SBE GEMS server to update touch screen instruction text files.

   The GEMS servers in Allegany, Dorchester, Montgomery, and Prince George's Counties are stand-alone servers connected to a closed network for loading touch screen memory cards prior to each election.

4. Reengineer Diebold source code to eliminate "hard-coded" passwords **Completed**

5. Implement cryptographic protocols for electronic transmission of data when using telecommunications facilities for data transfer **Completed**

6. Validate ballot storage randomization capabilities to prevent tracing ballots cast to individual voters **Completed**

7. Establish alternative process for ballot distribution to eliminate the potential vulnerability of communication intrusion **Completed**

8. Independent Testing Authority (ITA) review of Diebold source code **Completed**

9. Independent security review of Diebold source code **Completed**

10. Perform risk assessment when system changes are made **Completed** To ensure system changes do not negate existing security controls

11. Implement procedures to verify that the ITA certified version **Completed** of software and firmware is loaded prior to implementation (including forward-date checking for "Trojan horse" code)

12. Implement password policy and procedures **Completed**

13. Implement general support system procedures regarding appropriate access controls to the system. **Completed**

14. Implement additional security logging and auditing capabilities **Completed**

15. Implement identification and authentication procedures (including unique user ID and password) **Completed**

<u>Phase II</u>

16. Develop and implement information security awareness training program **Completed**

17. Hire SBE Chief Information Systems Security Officer **Completed** and two support personnel

18. Award contract for personnel to assist in developing ISSP **Completed**

19. Develop process and frequency of audit log review **Completed**

20. Develop and implement a formal, documented process to detect unauthorized transaction attempts by authorized and /or unauthorized users **Completed**

21. Implement a formal security change control process **Completed**

Phase III

22. Implement audit process for validating LBE compliance with the ISSP **Completed**

23. Validate existing procedures for 100% verification of electronic transmissions at LBE **Completed**

Completion of all 23 required actions **Completed March 31, 2004**

Implementation of a formal Information System Security Plan (ISSP) for all SBE Information Technology Systems **Completed June 30, 2004**

RECOMMENDATION

CONTINUE WITH THE IMPLEMENTATION OF PHASE II OF THE DIEBOLD CONTRACT

Continue with the implementation of Phase II of the Diebold contract, while requiring Diebold to make changes to the AccuVote-TS voting system and implement the updated system in 19 new jurisdictions and existing 4 jurisdictions by March 2004 Primary.