
**A Review of Issues Relating to the Diebold
Accuvote-TS Voting System in Maryland**

**Presented to the
Senate Education, Health, and Environmental Affairs Committee
and
House Ways and Means Committee**

**Department of Legislative Services
Annapolis, Maryland**

January 2004

For further information concerning this document contact:

Department of Legislative Services
90 State Circle
Annapolis, Maryland 21401

Baltimore Area: 410-946-5400/5410 – Washington Area: 301-970-5400/5410

Other Areas: 1-800-492-7122, Extension 5400/5410

TTY: 410-946-5401 – 301-970-5401

TTY users may also use the Maryland Relay Service to contact the General Assembly

E-mail: libr@mlis.state.md.us

Home Page: <http://mlis.state.md.us>

The Department of Legislative Services does not discriminate on the basis of race, color, national origin, sex, religion, or disability in the admission or access to its programs or activities. The department's Information Officer has been designated to coordinate compliance with the nondiscrimination requirements contained in Section 35.107 of the Department of Justice regulations. Requests for assistance should be directed to the Information Officer at the telephone numbers shown above.



DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF THE EXECUTIVE DIRECTOR
MARYLAND GENERAL ASSEMBLY

Karl S. Aro
Executive Director

January 29, 2004

The Honorable Paula C. Hollinger
Chairman, Senate Education, Health, and Environmental Affairs Committee
2 West, Miller Senate Building
Annapolis, Maryland 21401-1991

The Honorable Sheila Hixson
Chairman, House Ways and Means Committee
110 Lowe House Office Building
Annapolis, Maryland 21401-1991

Dear Chairman Hollinger and Chairman Hixson:

On October 20, 2003, you requested that the Department of Legislative Services (DLS) conduct an independent review of the issues flowing from the State's purchase of Diebold Election Systems' computerized balloting machines. On November 20, 2003, you expanded your request, asking DLS to examine and assess security and voting verification issues related to the use of the Diebold equipment and software.

More specifically, DLS was asked to examine and critique: the study conducted by Dr. Aviel Rubin (the Hopkins Study); the methodology used and the conclusions reached by SAIC regarding the integrity of the Diebold voting system; the process used to select SAIC to conduct the review of the Diebold system and the Hopkins report; and the overall security of Maryland's election procedures. DLS was also asked to comment on the budgetary and personnel history of the State Election Board as relates to these issues and to provide projections of increased budgetary and personnel needs based on the SAIC report. A review of internal administrative and technology controls of other executive agencies was also requested. Finally, with regard to security and voting verification, DLS was asked to assess several elements including the ability of an individual voter to verify the accuracy of the vote actually cast and whether the technology along with operations management processes provides election officials with the means to detect tampering.

As we moved forward with the project it became clear that DLS needed to engage outside resources to assist us in responding to your request. Consequently, we hired RABA Technologies, a Maryland technology company, in the capacity as a trusted agent to assist us with several aspects of the project relating to the review of the Hopkins and SAIC reports as well as the questions relating to the security and integrity of the Diebold voting system. The RABA team, headed by Dr. Michael Wertheimer, has proved to be an invaluable resource in this capacity, and its report is included as an integral part of the department's response to your request.

In addition to the RABA team, invaluable contributions were made by Michelle Davis, Simon Powell, Robert Koslowski, and Nelson Hopkins. I would also like to acknowledge the cooperation of the staff of the State Board of Elections and Diebold Election Systems, without whose cooperation DLS and the RABA team could not have completed its task.

Sincerely,

Karl S. Aro
Executive Director

Contents

Transmittal Letter	iii
Executive Summary	vii
Voting Equipment Overview.....	1
Voting Technology Vendors.....	1
Electronic Voting Technology	1
The Certification Process.....	3
Overview of Maryland Election Practices and Procedures with Respect to Direct Recording Electronic Technology	4
SBE Operational Practices.....	5
Process Used to Select SAIC to Conduct Review of Diebold Equipment and Hopkins Report.....	9
Review of Internal Administrative and Technology Controls in Other Executive Branch Agencies	11
OLA IS Audit Process and Standards	11
Recent DBM Actions	13
The RABA Report	15
The SAIC Report.....	16
The Red Team Exercise.....	17
Paper Ballot Receipts.....	19
State Board of Elections – Personnel and Funding Trends.....	21
Accessing Federal Funds	24
Funding Adequacy	25
Meeting Maintenance of Effort and State Match Requirements.....	26
Implementing the State Plan	27
Additional Spending Not Anticipated in the State Plan	30
Conclusions.....	32
Conclusions and Recommendations	33
Appendix	35

Executive Summary

The Department of Legislative Services (DLS) was asked to conduct an independent review of the issues flowing from the State's purchase and implementation of Diebold Election Systems' computerized balloting machines. To facilitate this review DLS used in-house resources and engaged the services of RABA Technologies, a Maryland technology company, in the capacity as a trusted agent to assist with several aspects of the project relating to the review of the Hopkins and SAIC reports as well as the questions relating to the security and integrity of the Diebold voting system.

The voting technology industry currently consists of four key vendors; Avante, Diebold Election Systems, Election Systems and Software (ES&S), and Sequoia Voting Systems. Of the four, two are private firms and two are subsidiaries of much larger corporations.

Modern touchscreen DRE's fall into two categories; full face and ATM style units. The functionality of the units is virtually identical however. This generation of DRE's is distinguished by software platforms that are compatible with windows operating systems. Both styles feature redundant and removable memory, the ability to present the ballot in different languages, and a removable memory card and a voter access card. This voter access card is a key feature of the touchscreen unit. A ballot cannot be cast on the unit unless an encoded voter access card is inserted. Election officials control the encoding mechanism and cards cannot be used to cast a ballot on the voting unit more than once until it is re-encoded.

Because Maryland is at the forefront of election reform, the SBE's election practices

and procedures with respect to DRE technology are difficult to compare with those of other states in most cases. Also, Maryland has advanced considerably in terms of its centralized administrative operations making it well positioned under the new federal regime of requirements under HAVA, which steers election management duties and responsibilities to states and away from local jurisdictions.

In June 2002 SAIC was competitively selected from the ISSS vendors by DBM for a task order to provide Statewide IT Security Support. The task order had a two-year term and included the performance of certification and accreditation reviews of State IT systems as well as other subtasks. On July 23, 2003 a Johns Hopkins University report on the Diebold Electronic Voting system was released, which led to the Governor ordering an independent review of the State's Diebold voting system. Due to the Governor's request and the tight deadlines involved with the implementation of the State's new Diebold voting system for the Spring 2004 presidential primary, DBM decided to have SAIC perform a risk assessment, an aspect of a certification/accreditation type review, on the voting system under the previously awarded task order.

OLA audit results show that poor security over computer systems is a widespread problem in Executive Branch agencies. At the December 2002 meeting of the General Assembly's Joint Audit Committee, OLA presented an analysis of the problems found during audits of 24 major state agencies over the previous 16-month period. OLA concluded that inadequate security is a pervasive problem. Many computer systems were not properly protected, which increased

risk. Unnecessary and/or unauthorized access to critical computer systems and files was identified at 21 of the 24 agencies.

The primary reasons identified by OLA for the computer security problems were the lack of overall security guidance from DBM (the State's IT oversight agency), the lack of emphasis on security during computer system design, and personnel turnover and vacancies.

RABA found the Hopkins report to be a thorough, independent review of the AccuVote source code and should be credited with raising valid issues that have resulted in considerable improvements. However, RABA also notes that if the authors had approached SBE, many of their erroneous assumptions about election processes could have been corrected and the discussion not weakened by a lack of understanding of those election processes.

The SAIC Report assessed risks to the AccuVote system with respect to three types of controls: Management; Operational; and Technical. The guidelines used in the SAIC report appear to be the result of internally generated requirements as developed over similar assessments combined with the State's general IT security and accreditation guidelines.

Because SAIC did not perform a thorough source code review, several of the requirements that are deemed to have been met rely on the presumed integrity of the Diebold software and the Microsoft operating systems. The SAIC Report also addresses the Hopkins Report's claims. RABA feels that the technical evaluation conducted by SAIC is lacking. Further, the SAIC Report relies on the integrity of the Diebold code as installed and the implemented security procedures. The SAIC Report does not account for the failure of any of these systems, nor does it provide any mitigation strategies for component failure,

especially at the software level.

The Red Team exercise was held on January 19, 2004. The purpose of such an exercise is to simulate the actual environment using the same equipment and procedures. The team is then free to "attack" the system. The team focused on smart card, AccuVote-TS terminal security, GEMS server security, and the methods used to upload results of an election. In each instance the team found vulnerabilities that could be exploited by malicious individuals. The team also has made recommendations to mitigate these vulnerabilities and it is important to recognize that official results are easily protected when these recommendations are implemented. Each finding, along with the recommendation to mitigate the attendant vulnerability is detailed in the RABA Report found in the Appendix.

Software changes are not needed before the March primary election in order to have a secure election. RABA has suggested several mitigation techniques that will significantly reduce the probability of a successful attack on the system. For example, the use of security tape to secure access to the voting terminals and the GEMS servers will discourage, if not prevent, tampering as well as provide a reliable means to identify any attempt at tampering.

The issue of the need for individual voter receipts as a means of providing a verifiable audit trail and to validate the accuracy of electronic voting systems is perhaps the most controversial issue in the debate over the integrity and security of these systems. RABA believes that a secure system without paper receipts can be built, but it would require not only better software, but also a higher level of sophistication and understanding by those who run our elections at the local level. One of the stated Federal Election Commission goals is to have less than

1 in 2 million votes counted incorrectly with electronic systems. Such accuracy has never been obtained with paper ballots. Ballots can be misread, smudged, lost stolen, destroyed, etc. Furthermore, voters cannot know how their paper ballots will be read; a properly configured electronic system provides this assurance. Currently, the Diebold system stores an image of each ballot cast. These can be downloaded from the memory cards and printed at the local board of elections for the purposes of conducting a recount.

There are a number of issues that will affect the SBE's need for additional resources. Depending on how they are resolved additional costs may be incurred. For example, most obvious potential cost relates to adding printers to voting machines in order to provide a hard copy voting record. Additional costs are anticipated for systems security, which includes training of local election officials and judges. Many of the recommendations made by RABA can be implemented at little or no cost, for example requiring that security patches and anti-virus software are up-to-date and installing passwords. However, some of the recommendations such as rewriting the software code in order to institute best security practices will require potentially significant expenditures (although it remains to be seen whether the State or Diebold will bear those costs). The cost of other recommendations is difficult to assess.

Voting Equipment Overview

Voting Technology Vendors

The voting technology industry currently consists of four key vendors; Avante, Diebold Election Systems, Election Systems and Software (ES&S), and Sequoia Voting Systems. Of the four, two are private firms and two are subsidiaries of much larger corporations. Diebold, ES&S and Sequoia have been in either the voting technology or automated computing market for decades. Diebold is a byproduct of the acquisition of Global Election Systems and ES&S is a product of a 1999 merger of American Information Systems and Business Records Corporation. Sequoia, which is currently a subsidiary of a British technology concern, began making paper ballots systems at the turn of the century. Avante is an up and comer in the voting technology industry. Its feature product is a touchscreen unit with a built-in paper receipt that can be viewed and verified by a voter before being rolled out of sight to maintain ballot secrecy.

In terms of market share, one voting industry representative characterized the three established firms as each having approximately 30% of the voting technology market while the remaining 10% is the domain of dozens of smaller competitors. **Exhibit 1** displays general corporate information obtained from official company websites and company officials directly.

Electronic Voting Technology

Modern touchscreen direct recording electronic (DREs) devices fall into two categories; full face and ATM style units. The functionality of the units is virtually identical however. The full-face touchscreen allows all races on a ballot to be displayed at once while the ATM-style units require users to page through election contests in order to vote. As one might expect, the full-face units have larger screens and are heavier than their ATM-style counterparts. This generation of DREs is distinguished by software platforms that are compatible with windows operating systems and that interface with the voter to cast a ballot. Both styles feature redundant and removable memory, the ability to present the ballot in different languages, a removable memory card, and a voter access card. This voter access card is a key feature of the touchscreen unit. A ballot cannot be cast on the unit unless an encoded voter access card is inserted. Election officials control the encoding mechanism and cards cannot be used to cast a ballot on the voting unit more than once until it is re-encoded.

**Exhibit 1
Voting Technology Industry
General Information**

	DIEBOLD ELECTION SYSTEMS	AVANTE INTL TECHNOLOGY	ES&S	SEQUOIA VOTING SYSTEMS
Ownership	Diebold	Private	Private	De La Rue (UK) maker of secure automated systems
Yrs. In Business	Diebold (1859) - Diebold ES (2002)	Founded (1982) Voting vendor since (2000)	35yrs	110yrs
Market Share	33,000 units	0	28,000 units	35,000 units
No. of Employees	13,000plus(Diebold)	50	400	300
Products/Industries	Automated Computer Systems for Retail, banking, Gaming, Pharmaceutical, educational institutions, government, and security applications.	Epoxies, Materials, and smart card Technology	Voting systems	Voting systems
Models	Accuvote-TS	Vote-Trakker EVC308-SPR	Ivotronic	AVC Edge
		Vote-Trakker EVC308-SPRFF		AVC Advantage (full face)
		Vote-Trakker EVC308		

Source: Department of Legislative Services

This generation of voting units makes the election process more versatile. Most units are capable of serving visually impaired voters and do not allow overvoting, which make up a substantial portion of uncounted ballots ¹. Similarly, modern touchscreens alert the voter when they have not voted for every contest, which reduces unintentional undervoting. Election administrators benefit greatly from the technology as well. Different ballot displays among various local jurisdictions may be more easily produced and transferred electronically to each local board before an election as a result of the software component of the system. Generally, the software for touchscreen systems provides total election management functions, from ballot design and voter interfaces, to election result tabulation.

The Certification Process

All types of voting systems, including punchcard, lever machines, optical scan and direct recording electronic systems are subject to a voluntary system of federal voting system standards (FVSS) to become qualified ². Vendors of voting systems must abide by these requirements to be eligible to sell their systems in those states that have adopted these standards established by the Federal Election Commission in 1990 ³.

In addition to the standards, there is a voluntary testing and certification program that is developed and administered through the National Association of State Election Directors (NASED). Through this program, NASED chooses independent laboratories referred to as "Independent Testing Authorities" (ITA's) to conduct testing to determine a voting system's compliance with the FVSS ⁴. The testing covers the entire voting system of a vendor, including hardware, firmware (software resident in a machine, such as programming on a read-only memory chip) and software for user interfaces. Upon successful completion of testing by an ITA, each separate component of a system receives a NASED qualified identification number. All tested components of a system and its technical documentation are kept in escrow by the ITA to ensure that the certified version of a system is not modified without first going through the certification process. ⁵

The Help America Vote Act of 2002 (HAVA) has created a new mechanism for establishing voting standards by requiring the newly created Election Assistance Commission (EAC) to provide for testing and qualification of voting systems. ⁶ To support the EAC's mandate in this regard, HAVA created three advisory bodies under the EAC; a 110-member Standards Board consisting of state and local election officials; a 37-member Board of Advisors consisting of experts from the government, science and technology sector and; a 15 Member Technical Guideline Development Committee chaired by the Director of the National Institute of Standards and Technology (NIST). NIST is charged with recommending voluntary voting system standards that will be reviewed by the two boards and the EAC. Currently, NASED and the FEC are transitioning the current regime of standards and certification to the recently appointed EAC.

Overview of Maryland Election Practices and Procedures with Respect to Direct Recording Electronic (DRE) Technology

Administrative practices and procedures generally combine management and operational controls to minimize the risk of voting technology failure or compromise. The required approach to developing these controls does not differ as much as one might think from controls used on the optical scan technology that most local jurisdictions used in Maryland before the State Board of Election's (SBE) purchase of touchscreen technology. Like optical scan machines, DREs record votes electronically, and have removable memory. The SBE established and modified several distinct phases of documented procedure and practices aimed at maintaining the control and accuracy of voting units: 1) certification and testing; 2) election day procedures; and 3) voter education.

State and Local System Testing

In total, Maryland's voting units have undergone four distinct levels of testing. First, national qualification is awarded to the final package of hardware and software from the vendor as described above. The remaining three levels of testing are performed at the state and local level under the SBE's directives. These consist of: 1) state certification compliance testing; 2) independent verification and validation testing; and 3) county logic and accuracy testing (L&A).

The SBE has established a body of state certification requirements in accordance with its rulemaking power.⁷ The final version of voting unit software is examined by an independent consultant for compliance with these state regulations.⁸ Upon successful completion of state certification testing, the SBE releases the software to be installed on the voting units. The next phase of testing is undertaken upon delivery of the actual voting units. This phase of testing, called "independent verification and validation (IV&V) testing" is performed by an independent security consulting firm, and is used to test the functionality of the entire voting system.⁹ These tests are performed in each county on a predetermined statistical sampling of the units.

The final phase of testing (logic and accuracy) is completed in the days preceding the election. This process involves configuring, testing, and preparing the voting equipment for an actual election. Local boards of election (LBE) are responsible for implementing this phase according to detailed procedures issued by the SBE in coordination with the vendor and performing the testing in a public area. In general, the L&A testing ensures that: 1) each voting unit is fully functional and free from mechanical problems; 2) each voting unit contains the appropriate ballot style; 3) results are being tallied accurately on each component of the voting system and; 4) results can be transmitted accurately to the election database on a local board of election's server. The dual purpose of the L&A procedure is to both ensure operating accuracy and load the correct ballot type onto the units in preparation for an upcoming election. Successful completion of the L&A process results in each voting unit being sealed and delivered to assigned precincts for election day.¹⁰

Election Day Procedure and Poll Worker Training

The SBE assumes responsibility for developing election day practices and procedures which aim to guard against administrative or operational error in the deployment of the voting units and potential fraud, voter error, or administrative mishandling during voting hours. These election procedures are provided in each local jurisdiction's election judge training manual, which list plain English procedures using simple checklists easily performed by election judges. This manual prompts election judges to ascertain the authenticity of the voting units in three separate procedures. Voting totals are checked in six separate procedures. That manual also provides for the proper handling of voter access cards. According to procedures for the voting unit judge, the judge is required to give each voter with a valid voter authority card received from the book judge, an encoded voter access card. In addition, the voting unit judge must observe the voter place the access card into the appropriate slot on the voting unit and explain to the voter that the access card must be returned after voting.¹¹

Pre-election procedures require election judges to verify that all the voting hardware has been assigned to their specific precinct and that the software loaded on the voting unit also corresponds to the precinct. Before voting begins, judges must verify that each voting unit has accumulated "zero" votes, and that the software displays the correct date, time, and other election information including ballot style. At the end of voting, judges must reconcile the exact number of individuals voting in a precinct between the software, the public counter on each voting unit, the number of voting authority cards returned, and the number of persons checked as voting on the precinct register.

Diebold also provides extensive training on the use of the Accuvote-TS to election administration officials, which includes a security component. In addition, training is provided by local election board staff with the assistance of Diebold personnel, to every election judge appointed to serve on election day using the uniform training and procedure manual.

SBE Operational Practices Compared to Other States

As of January 2003, the Election Reform Project reported 5 states with DREs in all or most of its local jurisdictions.¹² However, every state except one had in place first generation DREs which are not touchscreen technology, but instead mimic the interface of a lever machine. On these units, a lighted button is pushed to make a selection on the ballot. While votes are recorded electronically on these units, the units do not depend upon a computer operating system to record a ballot, nor are most of these units handicap accessible.

Georgia became the first state to purchase and conduct a statewide election on modern touchscreen units in 2002.¹³ Maryland was not far behind when it conducted elections in four local jurisdictions using the Accuvote-TS touchscreen unit in 2002 as well. Other states are in

various stages of considering and purchasing new voting technology but only Maryland and Georgia will likely conduct the presidential election using touchscreen technology statewide.¹⁴

Because Maryland is at the forefront of election reform, the SBE's election practices and procedures with respect to DRE technology are difficult to compare with those of other states in most cases. Also, Maryland has advanced considerably in terms of its centralized administrative operations making it well positioned under the new federal regime of requirements under HAVA, which steers election management duties and responsibilities to states and away from local jurisdictions. For example, states receiving federal funds under HAVA must: 1) adopt performance goals and measures for Local boards; 2) train local officials and poll workers, and; 3) develop a uniform statewide registration system. These requirements act to centralize election management responsibility at the state level. Similarly, Maryland's procedures for the management of statewide electronic voting technology are well beyond most other states by virtue of its early decision to purchase touchscreen technology.

Endnotes

- Note 1. The Caltech/MIT Voting Technology Project (2001). *Residual Votes Attributable to Technology: An Assessment of the Reliability of Existing Voting Equipment*. [Electronic version.]
- Note 2. The current standards are available online from the Federal Election Commission website at (<http://www.fec.gov/pages/vssfina/vss.html>).
- Note 3. The standards have been updated since 1990. A listing of the states that have adopted the standards is available on the Federal Election Commission website at (<http://www.fec.gov/pages/faqsvss.htm>).
- Note 4. Currently, there are two approved software ITA's according to the National Association of State Election Directors: CIBER, Inc., of Huntsville, Alabama and SYSTEST LAGS, LLC in Denver, Colorado. See National Association of State Election Directors (2003), *General Overview for Getting a Voting System Qualified*. [Electronic version].
- Note 5. National Association of State Election Directors (2003), *General Overview of Getting a Voting System Qualified*. [Electronic version].
- Note 6. 42 U.S.C. §§15481 et. Seq.
- Note 7. Election Law Article, §9-102 and COMAR 33.09.02.
- Note 8. The Maryland State Board of Election contracted with election consultant Britt Williams, professor at Kennesaw State University. Professor Williams was a contributing author of the current Federal Election Commission voting system standards and has been a consultant in the Georgia state certification process for over 30 years.
- Note 9. The independent security consulting firm is BSC, founded in 1996, with offices in Reston, VA and Anne Arundel County, MD. The firm specializes in information security; quality assurance and control; and verification and validation testing of computer systems.
- Note 10. Each voting unit seal is numbered and recorded. Election officials then verify the seal numbers before preparing the units for voting on election day. Any discrepancies in the seal number or evidence of tampering would require that the voting unit not be used for an election.
- Note 11. Maryland State Board of Elections (2004) State Board of Elections Judges Training Manual. [Electronic version].
- Note 12. A color-keyed map is available at the Center's website at (<http://www.Electionline.org>).
- Note 13. Election Reform Information Project and The Century Foundation (2003). *Primary Education: Election Reform and the 2004 Presidential Race*. [Electronic version].
- Note 14. Telephone Interview. Doug Chapin, Director, Electionline.Org. (January 15,

Process Used to Select Science Application International Corporation to Conduct Review of Diebold Equipment and Hopkins Report

The Science Application International Corporation (SAIC) was founded in 1969 by Dr. J.R. Beyster and a small group of scientists. It has become one of the largest research and engineering firms in the nation, with over 42,000 employees and with offices in over 150 cities worldwide. It recently reported revenues of almost \$6 billion.

The Department of Budget and Management's (DBM) selection of SAIC, which was already under contract to perform information technology (IT) system security reviews, was a reasonable method for quickly obtaining a risk assessment of the State's new voting machines.

In April 2001, SAIC was one of three vendors competitively selected to provide Information System Security Support Services (ISSS) under DBM's statewide Technical Service Procurement (TSP) contract. The TSP contracting process, which is in accordance with State Finance and Procurement Article, Section 13-402 of the Annotated Code of Maryland, speeds up IT procurements by providing State agencies with an available group of pre-selected contractors to perform a variety of IT services. Under the contract, the three ISSS vendors were pre-selected to bid on DBM approved task orders relating to state agency IT system security projects.

In June 2002 SAIC was competitively selected from the ISSS vendors by DBM for a task order to provide Statewide IT Security Support. The task order had a two-year term and included the performance of certification and accreditation reviews of State IT systems as well as other subtasks valued at approximately \$2.6 million. In January 2003, the task order was amended to allow DBM the flexibility to select what steps of the certification and accreditation process to perform and which IT systems to review.

DBM personnel advised that during 2003 DBM began the process of selecting State systems that it would consider having SAIC review for certification and accreditation. On July 23, 2003 a Johns Hopkins University report on the Diebold Electronic Voting system was released, which led to the Governor ordering an independent review of the State's Diebold voting system. Due to the Governor's request and the tight deadlines involved with the implementation of the State's new Diebold voting system for the Spring 2004 presidential primary, DBM decided to have SAIC perform a risk assessment, an aspect of a certification/accreditation type review, on the voting system under the previously awarded task order. Specifically, SAIC was tasked by DBM to perform a risk assessment of the voting system's manual and automated processes and controls and make recommendations for any significant risk areas noted. SAIC's review was limited strictly to a risk assessment and did not formally certify or accredit the voting system.

Review of Internal Administrative and Technology Controls in Other Executive Branch Agencies

As required by State Government Article, Section 2-1221 of the Annotated Code of Maryland, the audit responsibilities of the Office of Legislative Audits (OLA) include audits of information systems (IS). Using guidance from a number of authoritative sources to evaluate agencies' IS operations, OLA's audits have found that poor security over computer systems is a widespread problem in Executive branch agencies. Until recently, OLA's audits have been the only systematic and comprehensive process for assessing IT controls at State agencies by an independent party.

OLA IS Audit Process and Standards

OLA has a dedicated team of IS auditors responsible for conducting IS audits at least once every three years at state agencies with major computer operations. The scope of IS audits primarily consists of evaluating general controls – the structure, policies and procedures that apply to an agency's overall computer operations. General controls are evaluated with respect to: the organizational management structure, segregation of incompatible duties (such as programming and computer operations), access to computer programs and data, physical access to computer facilities, and software program changes. When significant to an agency's operations, security over network communications is also reviewed. All audits are conducted in accordance with generally accepted government auditing standards.

The criteria, standards and audit procedures used in OLA's evaluations of IS general controls are based primarily on the United States General Accounting Office's (GAO) publication – *Federal Information System Controls Audit Manual*. The publication is used by GAO to audit Federal IS and by a number of state audit agencies. This audit guidance is supplemented by other criteria such as State internal policies established by the Department of Budget and Management, especially in the area of IS security.

OLA's evaluation of agency network communications consists of assessing how well an agency is protecting its critical network data from internal or external (such as the Internet) security threats. The criteria and audit procedures used vary, but consist of best practices gleaned from a number of industry-recognized authoritative sources, training manuals and other audit organizations.

Since the approach used to evaluate IS controls, including security issues, depends on many factors unique to individual systems, there is no single authoritative source or prescriptive process for conducting IS audits. Consequently, the auditor must determine, based on the circumstances, the criteria, standards and audit procedures that should be used for each IS audit.

For these reasons, it would not be practical for OLA or any other audit organization to exclusively use the security standards developed by SAIC for its review of the State Board of Elections (SBE). Those standards represent a compilation of criteria, some of which are uniquely suited to SBE's operations. The sources for the standards are the Federal Election Commission guidelines and Code of Maryland Regulations requirements, as well as best practices developed by SAIC. While some of these standards may be applicable to other state agencies, many apply only to SBE's computer applications and systems.

OLA IS Audit Results

OLA audit results show that poor security over computer systems is a widespread problem in Executive branch agencies. At the December 2002 meeting of the General Assembly's Joint Audit Committee, OLA presented an analysis of the problems found during audits of 24 major state agencies over the previous 16-month period.

OLA concluded that inadequate security is a pervasive problem. Many computer systems were not properly protected, which increased risk. Unnecessary and/or unauthorized access to critical computer systems and files was identified at 21 of the 24 agencies. Proper access controls are necessary to protect computer data from being read, altered or deleted by inappropriate persons. Also, many agencies did not have good disaster recovery plans for addressing major service disruptions.

The primary reasons identified by OLA for the computer security problems were the lack of overall security guidance from DBM (the State's IT oversight agency), the lack of emphasis on security during computer system design, and personnel turnover and vacancies. For example, OLA reported that only 2 of 18 critical IT positions at DBM were filled and there has been turnover in the State's Chief Information Officer position.

OLA suggested that the statewide security policy be issued as soon as possible. (The security policy was later issued in June 2003.) OLA also suggested that DBM develop statewide training on security issues, and attempt to fill and retain qualified staff who oversee IT security.

OLA audits do not cover the proprietary computer systems of third parties who are contracted by the State to provide data processing services. The contracting State agencies are responsible for obtaining system integrity assurance from such contractors. OLA audits of agencies using third parties for major computer applications include an assessment of the agencies' efforts to obtain such assurances.

Recent DBM Actions

Until recently, OLA's audits were the only systematic and comprehensive evaluations being performed of Executive Branch computer system controls by an independent party. However, under the State's Technical Procurement Services contract, DBM has awarded a task order to a contractor (SAIC) to begin performing certification and accreditation reviews of a few selected information systems. The reviews will use DBM's *Statewide Security Support IT Security Certification and Accreditation Guidelines* which delineate the process for conducting the reviews. The guidelines do not establish the specific security requirements for systems to obtain certification and accreditation; rather, the requirements are uniquely established for each review. We were advised that after its review at SBE, the contractor had initiated a certification and accreditation review of a DHMH network system.

The RABA Report

The Department of Legislative Services entered into an agreement with RABA Technologies, LLC to perform a trusted agent evaluation of certain issues surrounding the use of the Diebold election system in the upcoming elections. More specifically DLS requested that RABA:

1. Examine and critique the study conducted by Aviel D. Rubin, known as the Hopkins study.
2. Examine and critique the methodology and practices used by SAIC in its review of the Diebold equipment and the Rubin report.
3. Examine and critique the conclusions reached by SAIC regarding the integrity of the Diebold voting machines and the overall security of Maryland's election procedures.
4. Examine and critique the IT Security Certification and Accreditation Guidelines as issued by the Maryland Department of Budget and Management.
5. Assist DLS in comparing existing SBE practices and procedures to those of the counterparts in other states.

After reviewing the Hopkins study and the SAIC evaluation, RABA suggested that the Diebold election system, known as the AccuVote-TS Voting System (AccuVote), should be subjected to a "red team" exercise to determine what kinds of vulnerabilities, if any, exist. This exercise is designed to simulate the environment of an actual election by using the same equipment and procedures and allowing a team of experts to experiment with various attack scenarios.

This section summarizes selected RABA findings with respect to its evaluation of the Hopkins report, the SAIC report, and the Red Team Exercise. RABA's full report is appended to this document.

The Hopkins Report

RABA generally agrees with the conclusions of the Hopkins Report on purely technical matters. In its opinion, RABA states that the single most relevant finding by Dr. Rubin is the general lack of security awareness as reflected in the Diebold code.

While Dr. Rubin concluded that the only solution to the problem of an election depending upon the correctness, robustness, and security of the software in the voting terminal is to introduce a voter-verified voter trail, RABA points out that there is considerable debate on this point. RABA notes that "if the software, processes, and procedures of an all-electronic system are implemented robustly, if the source code and the operating systems are subject to rigorous testing, and if the security model is continuously and accurately updated it is theoretically possible to drive down the risk to the point that the introduction of voter verifiable receipts is counterproductive."

RABA agrees with Dr. Rubin that security through obscurity is not sufficient to protect a computer based system and that the assumption should always be that all components of such a system are publicly known. This is not to say that making these components public is good practice, but proprietary concerns should not be allowed to mask security through obscurity.

In summary, RABA found the Hopkins report to be a thorough, independent review of the AccuVote source code and should be credited with raising valid issues that have resulted in considerable improvements. However, RABA also notes that if the authors had approached SBE, many of their erroneous assumptions about election processes could have been corrected and the discussion not weakened by a lack of understanding of those election processes.

The SAIC Report

The SAIC Report assessed risks to the AccuVote system with respect to three types of controls: Management; Operational; and Technical. The guidelines used in the SAIC report appear to be the result of internally generated requirements as developed over similar assessments combined with the State's general IT security and accreditation guidelines. RABA finds the lack of rigorous guidelines by the Federal Election Commission or the National Association of State Election Directors to be troublesome. It also notes that the FEC Voting Systems Standards, as approved April 30, 2002, did not appear as explicit requirements in the SAIC Report.

The SAIC Report identified and completely evaluated 169 management baseline security requirements. Of these 35 were labeled as either partially unmet or unmet. SBE has taken action to rectify them all; however, documentation of these actions is not in an easily reviewable form.

There are 110 operational baseline requirements, 15 of which are labeled as partially unmet or unmet. RABA agrees that the key operational needs are security awareness training for election site officials, well documented procedures for maintaining integrity of all hardware and software systems, and the ability to detect and recover from security breaches in a timely manner.

Of the 47 technical baseline security requirements, 15 are labeled as partially unmet or unmet. Because SAIC did not perform a thorough source code review, several of the requirements that are deemed to have been met rely on the presumed integrity of the Diebold software and the Microsoft operating systems.

The SAIC Report also addresses the Hopkins Report's claims. RABA feels that the technical evaluation conducted by SAIC is subpar. Further, the SAIC report relies on the integrity of the Diebold code as installed and the implemented security procedures. The SAIC Report does not account for the failure of any of these systems, nor does it provide any mitigation strategies for component failure, especially at the software level.

The Red Team Exercise

The Red Team exercise was held on January 19, 2004. The purpose of such an exercise is to simulate the actual environment using the same equipment and procedures. The team is then free to "attack" the system. At the outset, the team developed attacks without reviewing the Diebold source codes. Once that step was completed more sophisticated attacks were planned with knowledge of those codes. The team focused on smart card, AccuVote-TS terminal security, GEMS server security, and the methods used to upload results of an election.

The team found vulnerabilities that could be exploited by malicious individuals with respect to the AccuVote-TS terminals, the GEMS servers, and the method of uploading results. The team also has made recommendations to mitigate these vulnerabilities. Each finding, along with the recommendation to mitigate the attendant vulnerability is detailed in the RABA Report found in the Appendix.

Paper Ballot Receipts

The issue of the need for individual voter receipts as a means of providing a verifiable audit trail and to validate the accuracy of electronic voting systems is perhaps the most controversial issue in the debate over the integrity and security of these systems.

RABA Technologies commented on this issue in its report reviewing the security and integrity of the Diebold AccuVote-TS election system. Although they may be found in the RABA report, RABA's comments and recommendations on voter paper receipts are reproduced below:

"Many have advocated the use of paper receipts as a way to provide an audit trail and to validate the accuracy of the electronic systems. This debate cannot be held without considering the basic need for voter trust in the system. While it is our belief that a secure system without paper receipts can be built, it would require not only better software, but also a higher level of sophistication and understanding by those who run our elections. It may never be possible to administer 16,000 autonomous touch screen terminals, 44+ servers, 32,000 locks and keys, thousands of voter cards, administrator cards, and security key cards with perfect fidelity. As this report indicates, there are many issues to address.

On the other hand, one of the stated Federal Election Commission goals is to have less than 1 in 2 million votes counted incorrectly with electronic systems. Such accuracy has never been obtained with paper ballots in any instantiation. Ballots can be misread, smudged, lost, stolen, destroyed, etc. Furthermore, voters cannot know how their paper ballots will be read; a properly configured electronic system provides this assurance. Thus, the introduction of paper receipts will almost certainly cause a discrepancy between the tallies. Whatever method is chosen to arbitrate this discrepancy, it is certain that accuracy between votes cast and votes counted will suffer.

In discussions amongst the team members, there was no single consensus recommendation, except that the introduction of voter-verifiable paper receipts is absolutely necessary in some limited form. The number of software vulnerabilities such receipts mitigate, the amount of savings they introduce by lowering the procedural requirements, and the trust they garner are likely to be just as cost effective in the long run as a fully locked-down all-electronic system.

However, we do not see the need to install such receipts on every device. Indeed, if all AccuVote-TS terminals are checked to ensure they are functioning correctly before an election, and if they are loaded with identical, digitally-signed, software which is checked both before and after an election, one can make the case that reconciling the results of a single, randomly selected, terminal with its paper receipts is sufficient to believe that the overall electronic counts in that precinct are accurate. Thus, if all the terminals are software and hardware enabled for receipts, one need only provide receipts for a small number of randomly chosen machines. Voters might even be given the choice of using such a terminal – or not."

Note that RABA makes this recommendation with the caveat that a number of recommended software changes are implemented. These changes are detailed on page 24 of the RABA report.

DLS believes that, in addition to the RABA recommendations, it is important to also consider the following when discussing the issue of paper receipts. First, any paper receipt that is would be considered an official election document must be kept secure and secret. This means that these receipts would have to be handed in, presumably with the voter's access card. These will have to be handled with the same degree of security that the DRE memory cards and printed vote accumulation for each DRE are now.

Second, the federal Election Assistance Commission has not yet issued regulations regarding the form and content of paper ballot receipts. Federal standards are expected to be issued by the end of calendar year 2004. Without federal standards there can be no guarantee that any receipt developed and implemented before the standards are issued would pass muster. This could add additional expense to the State. However, if requiring that a paper ballot receipt must be part of the electronic voting system is determined to be a significant means of increasing voter confidence in the integrity of the electronic voting system, then the implementation of such a receipt should be undertaken, notwithstanding RABA's concerns that the "introduction of paper receipts will almost certainly cause a discrepancy between the tallies." It should be noted that the current system allows the data on the memory cards to be loaded into the GEMS server and each individual ballot image printed for use in a recount. This is how the recount in Allegany County was done after the last general election.

Third, it is not feasible, even if the software and hardware for producing paper ballot receipts currently existed in the system, to implement the changes that would be necessary for the primary and general elections to be held this year. In fact, while the SBE should be able to implement many of the low-tech risk mitigation recommendations, it will be hard pressed to implement even a few of the software and hardware configuration recommendations suggested by RABA.

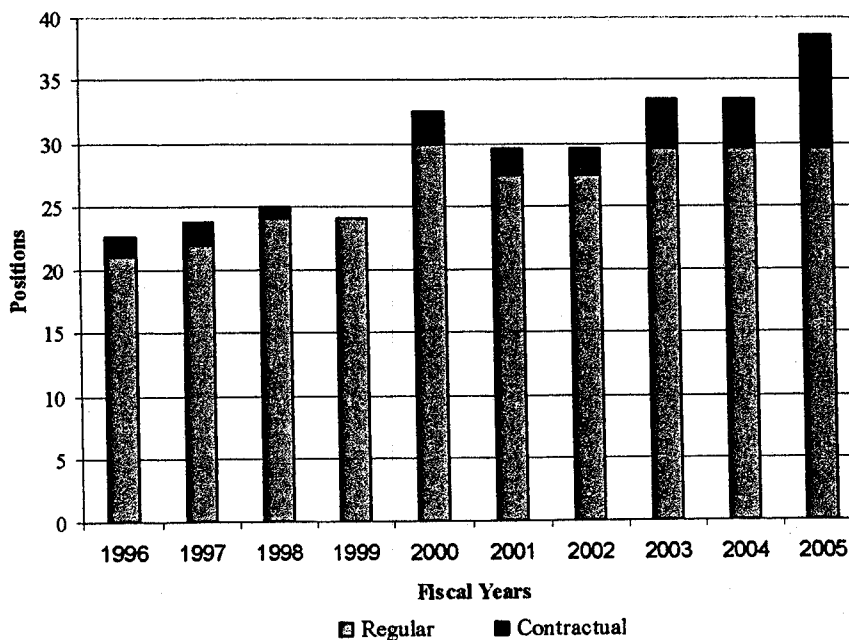
Fourth, the election results that will be transmitted from precincts to local boards of election are not official results. The official results are those that are found on the DREs' memory cards. Election procedures require that the election results on those cards be printed and bundled with the memory cards for transport to the local election boards. The software in AccuVote-TS DREs has been shown to count accurately. Assuming that the integrity of the DREs has not been compromised, the official election results will be able to be compiled at the local boards of election with an assurance of accuracy. The risk to election credibility arises if a malicious agent has been able to alter the unofficial results that are transmitted electronically to an extent that when the official results are tallied and released there is wide discrepancy between the two or that it appears an election result has been changed.

State Board of Elections Personnel and Funding Trends

The State Board of Elections (SBE) (under its prior name the State Administrative Board of Election Laws) was created through legislation in 1969. The administrative structure of the agency remained relatively unchanged until the 1998 session when the election code was revised. That revision strengthened the rule-making authority of SBE over the conduct, administration, and financing of elections.

As shown in **Exhibit 1**, that enhanced responsibility was matched by an increase in personnel resources made available to the board in fiscal 2000. Specifically full-time positions were added for information technology, campaign finance reporting, and fiscal support. Contractual support also increased. Two more regular positions (and additional contractual support) were added in fiscal 2003, again related to information technology support. At this point, SBE was responding to State legislation passed in the 2001 session (Chapter 564, Acts of 2001) mandating a uniform statewide voting system.

Exhibit 1
State Board of Elections Personnel Trends
Fiscal 1996 through 2005 (FTE)

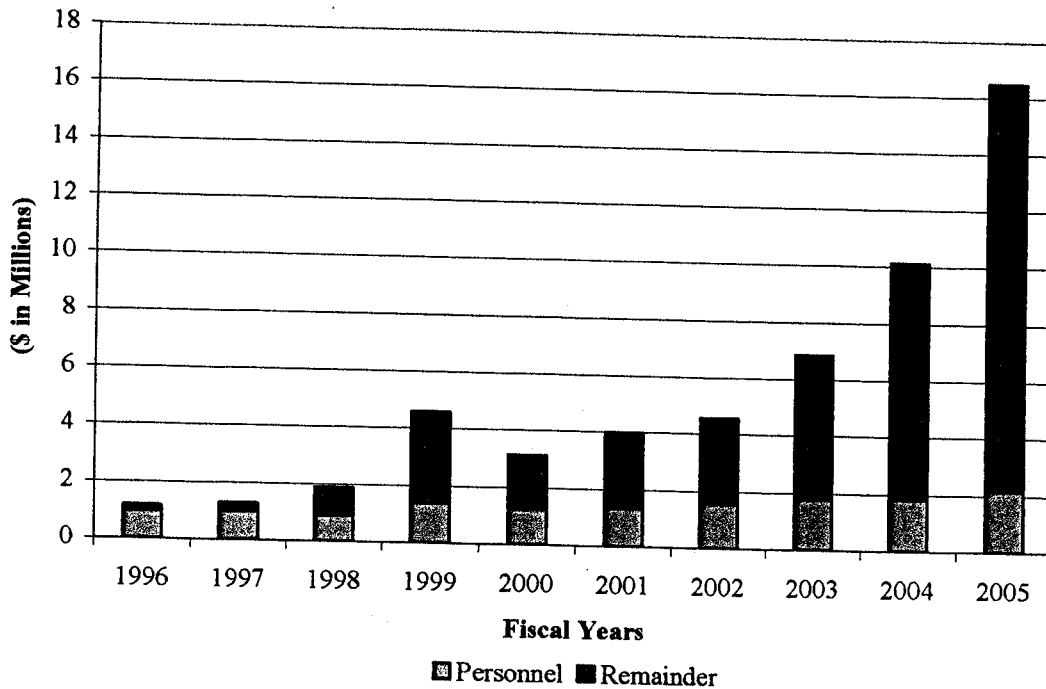


Source: Department of Legislative Services; Department of Budget and Management.

Although the Governor's fiscal 2005 allowance does not contain additional regular positions, 5 FTE contractual positions are proposed, all relating to federal Help America Vote Act (HAVA) implementation and supported through HAVA federal funds.

While resources for personnel have certainly been made available to SBE in recent years, personnel expenditures are increasingly a smaller percentage of its budget. As shown in **Exhibit 2**, personnel expenditures accounted for over 80 percent of SBE's budget in fiscal 1996. Although expenditures on personnel have more than doubled between fiscal 1996 and the fiscal 2005 allowance (an annual average growth of 9 percent), growth in the overall personnel complement has not been far behind, increasing from 22.58 to 38.5 FTE (an annual average growth of 6 percent).

Exhibit 2
State Board of Elections Funding Trends by Expenditure Type
Fiscal 1996 through 2005
(\$ in Millions)



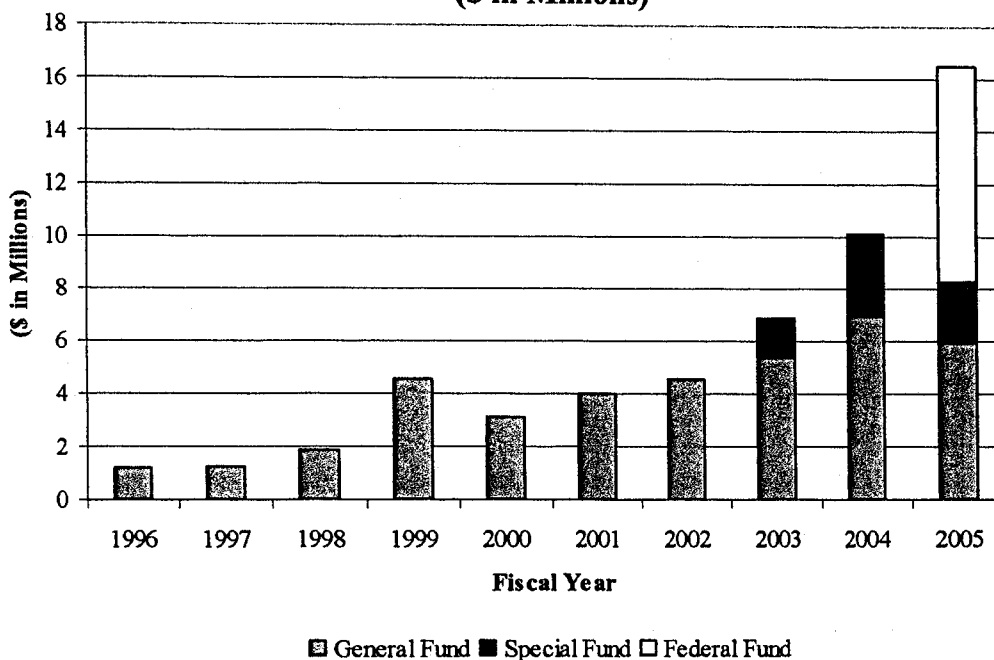
Source: Department of Legislative Services; Department of Budget and Management.

However, since fiscal 1998, the budget growth experienced by SBE between fiscal 1998 and the fiscal 2005 allowance (an average annual growth of 34 percent) has been driven by expenditures related to the modernization of the election system. This began with the passage of

the 2001 State legislation requiring the implementation of a uniform Statewide voting system and has been more than reinforced with the passage of HAVA in 2002. Communications costs, the use of contractual services, and equipment purchases have all increased dramatically.

Just as the spending levels have changed dramatically in recent years, so has the funding mix. As shown in **Exhibit 3**, from fiscal 1996 through fiscal 2002, SBE was almost always supported wholly through general funds. This changed in fiscal 2003 as local jurisdictions began to be charged for their share of the acquisition and operational cost of the uniform statewide voting systems required by Chapter 564. By fiscal 2004, just under one-third of SBE's budget was locally-generated special funds.

Exhibit 3
State Board of Elections Trends in Fund Sources
Fiscal 1996 – 2005
(\$ in Millions)



Source: Department of Legislative Services; Department of Budget and Management.

While a uniform statewide voting system is not a requirement of HAVA, the passage of HAVA in 2002 was certainly consistent with the State legislation and that local contribution is expected to continue. However, beginning in the fiscal 2005 allowance, the availability of federal funds under HAVA transforms the funding mix. Half of SBE's budget is anticipated to be federal funds in fiscal 2005 with general funds now only a little more than one-third of the total budget.

Accessing Federal Funds

As part of HAVA, significant federal funds have been made available to States. As shown in **Exhibit 4** Maryland is currently expecting to receive just over \$60 million in federal fiscal 2003 through 2005. Of this amount, almost \$7.3 million are Title 1 funds for improvements in election administration (just over \$5.6 million) and replacement of punch-card or lever voting machines (just over \$1.6 million). These funds, allocated respectively according to the State's voting age population as a percent of the national voting age population and the number of precincts that had obsolete voting machines, have already been received by the State. Title 1 funds did not have any matching or maintenance of effort requirements attached to them.

Exhibit 4 Anticipated HAVA Funds (Federal Fiscal Year)

	<u>Title 1</u>	<u>Title 2</u>	<u>Total</u>
2003	7,274,340	15,160,000	22,434,340
2004		26,820,000	26,820,000
2005		10,840,000	10,840,000
Total	7,274,340	52,820,000	60,094,340

Source: State Board of Elections

Title 2 funds, so called requirements payments, are the major source of federal funding and are available to implement the key requirements of HAVA (including requirements for voting systems, provisional voting and voting information, and voter registration) plus other approved election activities. At this time Maryland anticipates receiving \$52.8 million in Title 2 funds. As shown in Exhibit 4, these funds are anticipated over three federal fiscal years but none have yet been received by the State:

- Federal year 2003 funds have been appropriated but are not yet available for distribution. These funds must be distributed by the Election Assistance Commission (EAC) created by HAVA. The members of that Commission were not approved until November 2003 and currently are without office space and the funds to publish notification of fund availability in the federal register. However, HAVA requires distribution of the funding within 6 months of the Commission's appointment.

- Federal fiscal 2004 funds were appropriated in the Omnibus Appropriation Bill that finally passed the U.S. Congress on January 22, 2004.
- Federal fiscal 2005 funds are as authorized by HAVA.

All of the federal HAVA funds are to be placed in a Special Fund held by the State Treasurer's office. Maryland created this fund, the Maryland Election Modernization Fund, through Chapter 197, Acts of 2003. Federal funds may be held in this fund and drawn down for qualified expenditures.

Title 2 funds come with a number of strings including the filing of a State Plan with the EAC. Maryland filed its plan in May 2003. The two key budget requirements are:

- A State match of 5 percent of the total amount of federal funds received for eligible Title 2 activities (taking into account the amount of the requirements payment and the match amount spent by the State). This match must be made in the year in which the federal funds are received.
- A maintenance of effort requirement based on State expenditures for election activities for which requirement payments may be used in fiscal 2000. In Maryland, the SBE has determined that this amounted to \$1,994,914. This amount was based on general fund expenditures for the Statewide Voter Registration System (an eligible activity for requirements payments) plus an indirect cost amount calculated as a percentage (39.4%) of other SBE expenditures. That percentage was determined based on the portion of the total SBE budget expended on the voter registration system in that fiscal year. The indirect cost percentage will vary according to the amount of general fund expenditures on eligible activities. The maintenance of effort requirement is in effect for as long as the State receives requirements payments.

In determining compliance with the match and maintenance of effort requirement in a particular fiscal year, the same calculation applies, i.e. direct expenditures on eligible activities plus appropriate indirect costs.

Funding Adequacy

One of the key questions facing the SBE is the adequacy of its budget to meet the requirements imposed by HAVA as articulated in the State plan. Certainly, as indicated above in Exhibit 4, the State does stand to receive a significant amount of federal funds. Clearly, the most immediate requirement for the State is that the SBE budget meets the maintenance of effort and matching requirements necessary to receive those federal funds. The longer-term question is how much of the State's anticipated expenditures will be covered by those federal funds.

Meeting Maintenance of Effort and State Match Requirements

The current fiscal 2004 working appropriation appears to meet both the maintenance of effort and matching requirements necessary to access federal HAVA funds.

- In fiscal 2004 the State match requirement has yet to be determined since no Title 2 funding has been received. As noted above, the State may expect to receive anywhere from \$15.16 million to \$41.98 million in fiscal 2004. The working appropriation provides for almost \$3.1 million in general funds for eligible Title 2 activities plus \$1.7 million in indirect costs for a total of \$4.8 million, more than satisfying the matching requirement for any amount of federal funds to be received.
- Similarly, the \$4.8 million in eligible State expenditures that can be counted against maintenance of effort exceeds that requirement.

The fiscal 2005 allowance also appears to more than meet both requirements:

- In fiscal 2005 the State is anticipating the receipt of \$10.84 in federal funds. The allowance provides for almost \$1.8 million in general funds for eligible Title 2 activities plus \$1.3 million in indirect costs for a total of almost \$3.1 million, more than satisfying the match requirement. Even if the State receives the \$26.82 million in federal fiscal year 2004 funds in State fiscal year 2005 the match is still met.
- Similarly, the \$3.1 million in eligible State expenditures that can be counted against maintenance of effort exceeds that requirement.

Implementing the State Plan

Beyond satisfying funding requirements necessary to receive federal dollars, are the available funds adequate to implement the State Plan? The various components of the State Plan and the deadlines for meeting those components are shown in **Exhibit 5**.

Exhibit 5 State Board of Elections Key HAVA Requirements and Implementation Deadlines

<u>Deadline</u>	<u>HAVA Requirement</u>	<u>Status</u>
January 2004	Provisional Voting	Complete
	Voting information requirements	In progress
	Statewide Voter Registration List	Extension requested (1/2006)
	Computerized list maintenance	Extension requested (1/2006)
	Verification of voter registration info.	Extension requested (1/2006)
	Mail voter registration	Complete
	Military/Overseas voting	Complete
November 2004	Replacement of punchcard/lever machines	Complete
January 2006	Voting system standards	In progress
	Alternative language accessibility	Complete
	Vote standardization	Complete
January 2007	Voting system accessibility	In progress
On-going	Voter education and outreach	
	Training for election officials and judges	
	Voter accessibility improvement	

Source: Department of Legislative Services, State Board of Elections

Although as shown in Exhibit 5 the State faces numerous deadlines in the next three years, spending both to meet those deadlines and then to maintain compliance with HAVA will be ongoing. For example, because SBE has financed the purchase of voting machines from Diebold through lease agreements financed through the State Treasurer's office, SBE will be making lease payments through fiscal 2014. Similarly, the same contract that SBE has with Diebold to provide voting machines includes maintenance and services through calendar 2008.

Exhibit 6 provides detail on known costs anticipated for implementation of the State Plan, other HAVA-related expenditures that have been charged to HAVA funds, as well as an estimate for implementation projects for which costs have yet to be fully developed. Data includes the current fiscal year, the allowance, and known lease payment and contract (Diebold) costs.

Exhibit 6
State Board of Elections
Expenditures Associated with the Implementation of the State Plan
Fiscal 2004, Fiscal 2005, and Out-Year Requirements

<u>Item</u>	<u>Fiscal 2004</u>	<u>Fiscal 2005</u>	<u>Out-years Fiscal 2006-14</u>	<u>Total</u>
Hardware				
Lease Payments (Phase 1 and 2)*	\$5,034,100	\$9,654,583	\$38,407,457	\$53,096,140
Maintenance/Services				
Phase 1 and 2	5,559,554	3,515,168	18,991,290	28,066,012
Independent Verification and Validation (IV&V)	380,000			380,000
Contractual Staff**	75,460	316,331	TBD	391,791
Other HAVA Expenditures				
SAIC Report	169,212			169,212
Response to SAIC Report	558,714			558,714
Other State Plan Expenditures TBD:				
Statewide Voter Registration System				
Official and Pollworker Education and Training				
Miscellaneous Administrative Reforms				
Phase 3 Expenditures***				
Total Actual/Known Expenditures	\$11,777,040	\$13,486,082	\$57,398,747	\$82,661,869
Range of Future Expenditures TBD			\$15,000,000- 21,000,000	\$97,700,000- 103,700,000
Current Funding Levels				
General Fund	\$3,066,655	\$1,799,726		
Special Fund	3,146,764	2,284,875		
Federal Fund****	803,386	8,270,000		
Total	\$7,016,805	\$12,354,601		
<i>Difference</i>	<i>-\$4,760,235</i>	<i>-\$1,131,481</i>		

* Phase 1 counties were Allegany, Dorchester, Montgomery and Prince George's. Phase 2 counties are other jurisdictions except for Baltimore City which is Phase 3.

** Data for fiscal 2004 and 2005 are as per the current budget. It can be anticipated that this level of expenditures will be required for contractual support for the next several fiscal years.

*** Costs will increase if hardware requirements are financed.

**** For the purposes of this exhibit, federal funds for fiscal 2004 include federal funds for budget amendments submitted by SBE to the Department of Budget and Management but not yet approved. To date, only \$75,460 has been formally approved.

Source: Department of Legislative Services, State Board of Elections

A number of points can be made from this exhibit:

- The current working appropriation and Governor's allowance does not include sufficient funds to cover known obligations. While funding is available to cover the cost of lease payments to the Treasurer, insufficient funding exists to cover the remainder of the amount anticipated to be spent for maintenance and services. The shortfall is just over \$5.9 million for those two years. However, as noted in Exhibit 4, the State has already received almost \$7.3 million in HAVA funds and a further \$15.2 million has been appropriated at the federal level (though not yet received by the State). Thus, it can be assumed that these funds will be added to the budget by budget amendment to cover existing obligations. No additional State funds will be needed as the existing appropriation/allowance will more than cover the State match at that higher spending level.
- Total known expenditures levels from fiscal 2004 through current lease payment agreements are almost \$82.3 million.
- A significant amount of expenditures to implement the State plan have yet to be determined but may total between \$15 and \$21 million:
- Phase 3 hardware and maintenance/services costs (Baltimore City) are estimated at \$7.2 million (a figure that will increase if hardware costs are financed through a lease agreement as has been the case for phase 1 and 2 counties).
- The movement of the State's voter registration list onto a single centralized database is required by HAVA. The local election boards currently operate six separate voter registration systems. Based on the SBE's assessment of voter registration systems nationwide, there is no Commercial Off the Shelf (COTS) solution yet available. Project estimates are \$6-12 million.

- Again, while some official and pollworker training is included in the Diebold contract, other costs are anticipated.
- Similarly, SBE anticipates incurring additional administrative costs, potentially \$2 to 3 million.
- Some additional IV&V funding will be required.
- Contractual support will also add to out-year costs.
- This exhibit assumes no additional changes to the current election system or voting machines (discussed further below).

Clearly, the total cost for State Plan implementation is significantly above the cost estimates used in the State Plan submitted by the SBE in May, where plan expenditures were estimated at \$70 to 79 million. While the \$60.1 million in federal HAVA funds will cover the majority of initial funding needs, State and matching local funding will have to fill the gap.

In addition, beyond initial implementation, there will be significant ongoing maintenance and services requirements beyond the current Diebold contract. It can also be anticipated that the SBE will have a more extensive and permanent administrative structure. All this adds up to a significant ongoing expenditure of State funds for election activities at a higher rate than that currently provided for.

Additional Spending Not Anticipated in the State Plan

At this point, there are also a number of items not currently anticipated in the State Plan that may drive up expenditures (both one-time expenditures as well as ongoing expenditures):

- The most obvious potential cost relates to adding printers to voting machines in order to provide a hard copy voting record. When the new system is fully rolled-out, there will be approximately 17,600 voting machines statewide. Adding printers could mean expenditures for the printers themselves but also the cost of associated maintenance, services and training requirements. To date Diebold has not provided an estimate to add printers (not least because there is currently no approved standard for printers). Thus, although there is no clear estimate, adding printers to every machine could perhaps cost a minimum \$3.5 million.
- Additional costs are anticipated for systems security. The key recommendations of a Risk Assessment Report on the State's new voting system and processes undertaken by SAIC in response to criticism of the new system centered on the need to ensure the

integrity of the new system and develop a documented System Security Plan that made appropriate State and federal standards and industry best practices. The hiring of additional security staff was also recommended.

Other recommendations involved improvement of documentation and standardization of documentation provided to local boards of elections, improved documentation of a variety of processes at the State level, enhanced training at the local level, enhanced screening of election officials, and improved security standards at the SBE.

Some of these recommendations require the development and implementation of relatively straightforward policies and procedures at little cost. Other changes will require more extensive expenditures. As noted above in Exhibit 6, SBE has already anticipated spending \$559,000 responding to the SAIC report. Other expenditures are likely.

- It should also be noted that the Federal Election Commission (FEC) may impose additional requirements that involve increased expenditures. As noted in the RABA Technologies report on the State's new voting system, the FEC's current website includes a comment on the current standards that they are "not entirely" up-to-date and "the FEC is drafting the next version of the standards to cover the newer technology as well as to change standards that currently unduly restrict design."
- The RABA Technologies report provides a series of recommendations to improve the security of the State's voting system. Many of these recommendations can be implemented at little or no cost, for example requiring that security patches and anti-virus software are up-to-date and installing passwords. However, some of the recommendations will require potentially significant expenditures, for example rewriting the entire software code in order to institute best security practices. The cost of other recommendations is difficult to assess. For example, while RABA do not recommend adding printers to produce voter-verifiable paper receipts on every machine, depending on the number of machines that have the technology added, costs could be moderately high. In all cases, whatever changes are made will require additional training for election officials.

Indeed, one of the clearest messages to emerge from the RABA report is the need to have a more sophisticated cadre of election officials in order to implement improved security processes that must complement security measures that are being, and will continue to need to be, taken by SBE to develop and maintain the State's new voting system. Developing that cadre of officials will also be expensive.

Conclusions

Based on this review of SBE's budget, DLS concludes:

- Historically SBE has been provided with the personnel and fiscal resources to implement the modernization of the State's election system.
- SBE's fiscal 2004 working appropriation and fiscal 2005 allowance need to be supplemented by federal HAVA funds in order to meet current obligations.
- The attainment of federal HAVA funds is crucial to the implementation of SBE's State Plan and to date SBE has fulfilled the requirements necessary to receive those funds.
- The State's use of Federal HAVA funds will chart the course for future State general fund spending. Full implementation of the State Plan is estimated by DLS to cost at least \$97.7 to 103.7 million and changes to that plan including those recommended by RABA in its report (for example, enhanced security or additional hardware requirements) will add to that expense.

Certainly the HAVA funds offset the need for major State general fund expenditures in the short-term, even with the addition of expenditures beyond those currently known. However, at some point significant additional general fund expenditures will be required to cover long-term lease agreements and support the ongoing operation of the voting system that SBE is implementing. How the State uses those federal funds will determine when those additional general fund expenditures will be needed. However, barring additional federal funding, there is no doubt that the SBE will consume significantly more general funds resources in the future compared to its current budget.

DLS recommends that SBE present an updated expenditure proposal to the legislature for the implementation of the State Plan based on the recommendations of the SAIC report and also that of RABA Technologies. Since changes to the SBE budget and State election system may also be enacted during the 2004 Session, that update should be presented by July 1, 2004 to reflect any changes enacted by the legislature.

Conclusions and Recommendations

Based on the analysis by RABA Technologies and our own observation of the Red Team exercise, DLS believes that the March primary election can be held successfully without any changes to the Diebold software. The software accurately counts votes cast and has the ability to render a printed image of every ballot cast in the event that a recount is necessary. However, DLS also believes that it is critical to the success of the election that the State Board of Elections implement the physical security recommendations made by RABA with respect to the AccuVote-TS voting terminals and the GEMS servers. It is also imperative that SBE take steps to further train local election officials in basic security awareness with respect to the RABA findings.

DLS notes that the Diebold AccuVote-TS voting system has been used in four counties in the last statewide primary and general elections and in several municipal elections held in 2003. In every case the equipment performed as it was intended. After the general election a recount was conducted in Delegate District 1C. The recount also was conducted without difficulty.

Moving toward the general election, DLS recommends that SBE and Diebold work cooperatively to improve security in the system. While the physical security procedures should be sufficient in the short term, the recommendations with respect to system configurations and software should be taken seriously and every effort made to address these concerns before the November general election.

DLS recognizes that it is not possible to implement individual voter ballot receipts at this time and that it might be counterproductive to do so without clear federal standards. RABA points out in its report that it believes that a secure system without paper receipts can be built that will meet the Federal Election Commission's goal of having less than 1 in 2 million votes counted incorrectly. This degree of accuracy has never been reached with paper ballots. As an interim measure, with proper security procedures in place with respect to the AccuVote-TS terminals, it may be possible to equip only a limited number of the terminals in each precinct with the ability to provide voter receipts, check these receipts from randomly selected terminals against the electronic results, and be assured that the overall counts for a precinct are accurate. RABA points out that the introduction of voter receipts will almost certainly create discrepancies in the tallies, especially when introducing the human element. Voter confidence in the election system should be the primary objective; however, it is not clear that the implementation of individual voter ballot receipts is the only, or appropriate, solution.

Based on our review of SBE funding and personnel trends, DLS recommends that SBE present an updated expenditure proposal to the General Assembly for implementation in the State Plan based on the recommendations of the SAIC and RABA reports. Because it is possible that changes to the SBE budget and State election system may be enacted during the 2004 Session, the update should be presented by July 1, 2004.

DLS further recommends that SBE work with the local boards to implement an on-going training program for election officials. RABA suggests that election administrators at the state and local levels should consider establishing a program of formal security training. Such certificate programs are offered by private sector organizations (e.g., SANS).