MEMORANDUM

Elections Subcommittee
Agenda Item No. 2(A)

TO: Honorable Chairperson Barbara Carey-Shuler, Ed.D. and Members, Board of County Commissioners

DATE: April 19, 2004

SUBJECT: Voter-Verifiable Paper Record Study

FROM: George M. Burgess
County Manager

In response to a Resolution introduced by Commissioner Morales and approved by the Board of County Commissioners, Supervisor of Elections Constance A. Kaplan has prepared the attached report.

Attachments

Memorandum

TO: George M. Burgess
County Manager

DATE: March 23, 2004

FROM: Constance A. Kaplan
Supervisor of Elections

Constance A. Kaplan

SUBJECT: Voter-Verifiable Paper Record Study

Introduction

In response to a Resolution introduced by Commissioner Morales and approved by the Board of County Commissioners, the Miami-Dade Elections Department and Department of Procurement Management (DPM) have conducted a study of the feasibility of procuring a system that would print an individual paper record of each vote cast for review and approval by a voter before he or she leaves the polling place. County staff sent a Request for Information (RFI – Attachment A) to numerous potential vendors and received 11 responses from the industry. The State of Florida has not certified any paper record system and is not actively in the process of doing so. This includes both stand alone printers that would attach to our existing units as well as integrated systems including printers as part of a new overall electronic voting system.

Everybody involved in the discussion regarding whether to implement new voter-verifiable paper record (VVPR) technology shares a common goal of providing the most free, fair and accurate elections possible. We are adamant about making our election process a source of pride for the County. For all of us, the ongoing discussions about paper receipts, and their potential advantages and disadvantages, revolve around *how* – not *whether* – to administer elections with the highest degree of integrity.

Responses from the Election Industry

Responses to the RFI indicate that the election equipment industry would be interested in providing paper record capacity to the County and is in the process of developing the capacity to do so. Of the 11 respondents, six have voting systems that can incorporate a paper record printing system. Three companies indicated that their printers could work with the County's Election Systems and Software (ES&S) system. Those companies are the VeriVote/hp Invent Partnership; Ferey; and ES&S. Two of those companies – VeriVote/hp Invent and Ferey – have paper record printer systems available for purchase.

Two matrices are attached (Attachment B). Matrix A compares complete electronic voting systems providing paper records of voters' votes, which would necessitate scrapping the County's current system in favor of a completely new, integrated system. Matrix B compares separate paper record printing systems that could be compatible with the County's existing system. Both matrices also provide per-unit cost estimates.

For complete electronic voting systems, those estimates range from $3,000 per unit (or $21.6 million to replace the County's 7,200 iVotronic units) to $4,000 per unit (or a total of $28.8 million). For standalone printers (the less expensive option), estimates range from a low of $155 per unit (or $1.1 million for enough printers to complement the County's 7,200 iVotronic units) by VeriVote/hp Invent to $800 to $1,200 per unit (or $5.7 million to $8.6 million) by iVotronic manufacturer ES&S. Those estimates do not include the cost of new software, retrofitting the County's current units and installing the new equipment, nor the costs of logistically redesigning the County's election process and recurring costs of new supplies such as paper and ink. Our vendor has not provided estimates for those costs.

Elsewhere in Florida

The Florida State Association of Supervisors of Elections (FSASE) has released a position paper (Attachment C) recommending against the use of paper receipts, citing various reasons from the integrity of the system as it exists to doubts as to whether paper receipts would improve the integrity of the election process. The FSASE also cites the fiscal implications of implementing such technology. I would never recommend against the implementation of such technology based primarily on fiscal implications.

South Florida's other large counties, Broward and Palm Beach, have also studied the implementation of paper record technology. Palm Beach's Supervisor of Elections has recommended against paper receipts, but the County Commission has expressed considerable interest in purchasing paper record printers and voted to approve such a purchase when feasible. Broward's commission directed the County Administrator to study the feasibility of implementing the new technology. The resulting report (Attachment D) recommended against doing so. That report is attached; the discussion in Broward continues.

While state election officials in other states such as Nevada and California have advocated or mandated the implementation of paper record technology, Florida Secretary of State Glenda E. Hood, who serves as Florida's top election official, has expressed more reservation about the quick introduction of such technology, as evidenced in the attached letter from her to Senator Bob Graham (Attachment E).

Elsewhere in the United States

The decisions by state election officials in Nevada and California to require paper records of votes on DRE machines by, respectively, fall 2004 and 2006, followed analyses by computer scientists alleging that DRE systems are susceptible to malfunction and fraud. The most widely reported of those analyses, by a team of researchers at Johns Hopkins University, (Attachment F). Additionally, several close elections conducted with DRE systems left candidates frustrated with the inability to conduct recounts using paper records of individual votes printed at the time those votes were cast.

In compliance with the 2002 Help America Vote Act (HAVA), Miami-Dade's ES&S system does generate paper a paper audit trail, but those paper records are not, as the computer scientists and other advocates of VVPR wish, printed at the time a vote is cast and verified by the voter. Again, many of the issues which are traditionally resolved during paper recounts – overvotes, undervotes and voter intent – no longer present themselves with Miami-Dade's DRE system. Still, the system does not completely fulfill the desires of the computer scientists and other advocates who prefer that a voter view and verify a paper record at the time a vote is cast.

The four principle authors of HAVA -- two Democrats and two Republicans, one each from the U.S. Senate and House -- have recently written a letter (Attachment G) expressing their concerns that a rush to implement VVPR technology could negate some of HAVA's most important benefits. Specifically, they are concerned that visual paper records would be a step backward for visually impaired voters who, for the first time ever, can now vote unaided, in complete privacy, using audio-equipped touch-screen units.

A number of other news articles and documents speaking to the advantages and disadvantages of VVPR are attached. We have attempted to make this sample of written material representative of different views, though it is by no means exhaustive; many more volumes have been written about this topic.

Conclusion

Given the timeframe and lack of state certification for any VVPR system, the feasibility of implementing such a system in Miami-Dade County in 2004 is highly questionable. The challenges associated with purchasing equipment for which no certification or standards existed are well documented, and I have concerns about allowing Miami-Dade to once again be a testing ground for new technology. Under mandate, Supervisors of Elections in Nevada will attempt to utilize VVPR technology in November 2004, and the Miami-Dade Election Department will closely monitor their experiences. Clearly, Miami-Dade community leaders advocating such technology are not alone, and the election equipment industry is quickly responding to this relatively new yet significant market demand. Undoubtedly, unforeseen challenges will present themselves in the handful of jurisdictions using VVPR this year, and should Miami-Dade choose to purchase equipment following those experiences, the County would have the opportunity to procure a system developed by vendors who have had a chance to learn from both the successes and shortcomings of the first-ever utilization of VVPR in the United States.

Attachments

cc: County Attorney's Office
Alina T. Hudak, Assistant County Manager

REQUEST FOR INFORMATION

"Electronic Voting System With Paper Record of the Voter's Vote"

and

"Paper Record of the Voter's Vote"

RFI # 15

Miami-Dade County is interested in obtaining information from qualified vendors regarding **Electronic Voting Systems (Direct Recording Electronic (DRE) with Touch Screen) that produces a paper record of the voter's vote and an independent (stand-alone) Paper Record Printer System compatible with the Elections Systems & Software, Inc. (ES&S) iVotronic 15" Voter Terminal (Version 7.5). Additionally, the County seeks cost information related to each solution.**

The County is conducting market research to identify technology that will:

OPTION 1: Provide Direct Recording Electronic (DRE) voting which uses touch screen technology and provides a paper record of the voter's vote.

OPTION 2: Provide print technology that will integrate with the County's iVotronic 15" DRE Voter Terminal, version 7.5 to produce a paper record of the voter's vote.

The County desires to receive responses to this inquiry by close of business on Friday, October 24, 2003. This **is not** a Request For Proposals (RFP), but a request of the marketplace for information to aid the County in determining the availability of electronic voting systems capable of producing a paper record of the voter's vote and the availability of systems capable of producing a paper record of the voter's vote that will interface with the County's existing iVotronic 15" Terminal system, version 7.5.

A. DEFINITIONS:

For the purposes of this Request For Information (RFI), the following definitions apply:

Electronic Voting Systems with Paper Record Printer System: Shall mean electronic direct recording equipment (DRE) touch screen voting system capable of producing a paper record of the voter's vote.

Paper Receipt Printer System: Shall mean an independent printer system that will interface with an electronic DRE touch screen voting system to produce a paper record of the voter's vote.

ADA Voters: Shall mean voters with physical limitations such as blindness or hearing impairment.

County or the County: Shall mean Miami-Dade County, Florida.

Elections Department: Shall mean the County's Elections Department.

B. BACKGROUND

The Miami-Dade County Elections Department serves a voting population of approximately 936,700 voters at 749 precincts. In 2002, the County purchased a turnkey DRE voting system with touch screen technology and new scan voting system technology. These systems were provided by Election Systems and Software, Inc. (ES&S). The County purchased 7200 DRE Units and 14 Scan Units that were used in the 2002 Primary and General Elections.

C. INFORMATION REQUESTED

Please provide the following information that will assist the County in identifying options for a system(s) that will produce a paper record of the voter's vote, specifically addressing the following:

PART A: Electronic Voting Systems (DRE with Touch Screen) that produces a paper record of the voter's vote:

1. Please describe your DRE and how it meets the needs of voters, including ADA voters.
   a) Is this system currently available for use?
   b) If not, what is the anticipated date for availability?
   c) Is there a system prototype being tested? If so, please state where and the results to date.
   d) Does the DRE system provide a means by which ADA voters can verify their vote?

2. Is your system certified by the State of Florida?
   a) If so, when was certification granted? (Please provide copy of certification)
   b) If not, are there plans to do so and in what time frame?

3. Provide specifics regarding how your system incorporates the capability to provide a paper record of the voter's vote.
   a) Is the paper record capability a function provided by a business partner or part of your developed system?
   b) If business partner provides the solution, please provide information regarding the business partner and the paper record capability integration methodology.

4. Describe your system's warranty; discuss any exclusions and/or limitations.

5. Describe system maintenance and support provided. Please discuss the technical support

available and list if such support is available at different levels; for example: 1st level (silver), 2nd level (gold) and 3rd level (platinum).

6. What is the life expectancy of the system?

7) Where and by whom is your system currently being used? Please provide contact information for reference.

8) Please provide the technical specifications of your system.

9) Please explain your training capabilities for:
   a) Poll workers
   b) Operations staff
   c) Warehouse staff
   d) Technical staff
   e) Administrative staff

10) Please provide estimated system cost(s).

11) Are you able to provide the County a demonstration of your system(s)?

PART B: Paper Record Printer System (stand alone)

1) Please describe your Paper Record Printer System and how it meets the needs of voters, including ADA voters.
   a) Is this system currently available for use?
   b) If not, what is the anticipated date for availability?
   c) Is there a system prototype being tested? If so, please state where and the results to date.

2) Is your paper record printer system compatible with Election Systems & Software's iVotronic 15" Voter Terminal, version 7.5?
   a) If not, can it be made compatible with Election Systems & Software's iVotronic 15" Voter Terminal, version 7.5?
   b) If so, will it be ADA compliant, and has it been fully tested with the iVotronic equipment used by Miami Dade County? If so, where and please provide reference information.
   c) Does your system require retrofits or additional equipment to be compatible with the iVotronic system like the one used by Miami-Dade County? If so, please explain.
   d) Is your paper record printer system compatible with other electronic voting systems (DRE with touch screen technology)? If so, which one(s) and provide information regarding:
      i) the system (manufacturer and model)
      ii) where being used and contact information for reference

3) Where and by whom is your system currently being used? Please provide contact information

for reference.

4) Please provide the technical specifications of your system.

5) Please provide estimated system cost(s).

6) Are you able to provide the County a demonstration of your system(s)?

Those vendors wishing to respond to this Request For Information (RFI) must do so by 2:00 P.M. on October 24, 2003. Vendors responding to this RFI, may be invited to a meeting with County staff for further discussions. Responses may be forwarded in writing or via e-mail to:

Fred Simmons, Jr., RFP Unit Manager
Department of Procurement Management
Miami-Dade County
111 NW 1st Street, Suite 1300
Miami, FL 33128

Email address: Fred@miamidade.gov
Phone No. (305) 375-4259

ATTACHMENT B

RFP No. 15: Matrix
Part A: Electronic Voting Systems With Paper Record of the Voter's Vote

RFI: Key Information	Populex	Alpha Data Services, Inc.	IVS, LLC	ES&S	TruVote International, Inc.	Bharat Electronics Limited	VeriVote & hp Invent (Partnership)	Vogue Election Systems, LLC	Voting Technologies International	Ferey	Sequoia Voting Systems
Electronic Voting System With Paper record	The PopulexSlate: A Digital Paper Ballot system	VRES touch screen voting system	*Inspired* Voting Machine: Not a touch screen. System developed for used by the blind; uses a video screen	Did not respond to Part A since MDC already uses the iVotronic DRE touch screen system	DRE system w/paper record-drop box concept; tel. call-up verification capability	Solution does not address RFI requirements	N/A	N/A: They are presenting their AutoMark product used by voters w/disabilities who would mark an optical ballot	VTI system uses the VoT printer: Uses standard computer components	Referenced the Select 100 system which uses the Real Time Ballot Printer (RBP) system but no info provided	AVC Edgew/3 options for paper ballot verification
System Availability	Currently available; not certified: Pre-production units available	Currently available	After NASED VSS certification anticipated 12/03	N/A	Currently being tested: No date specified	N/A	N/A	Being submitted for certification 12/04	Currently available	N/A	Available for use w/only current certifications-did not state which one(s)
System Certification(s)	No: Will pursue basedon the Co.'s interest in the system	Not certified by State of Florida	NASED VSS certification anticipated 12/03:	N/A	Version 1.0 NASED certified; Version 2.0 available ¾: Certified by State of Arkansas	N/A	N/A	None	Federally certified in 13 states	N/A	Not certified in FL
System being used?	Used for student body elections at Dundee Crown High School and the Middle School	No: Sales after certifications (Fed. & State(s)-2004)	Three prototypes being beta-tested	N/A	System was used by AKA Sorority and in a demo election in Lakewood, Tenn. (See video presented)	N/A	N/A	No	Indiana and South Caolina	N/A	Santa Clara Co., CA, Riverside Co., CA, Hillsborough Co., FL, and others

ATTACHMENT B

Technical Specs. Provided?	Yes	Minimal	Yes: Uses two types of bar-coded paper record receipts:	N/A	Yes	N/A	N/A	Minimal	Minimal	N/A	Yes: For hardware and software
Estimated Cost(s) Provided?	Non provided	Based on proposal	$4,000 for base unit: software and hardware additional; not priced yet	N/A	Approximately $3,000	N/A	N/A	Yes	Yes	N/A	Yes
Demo Recommended?	No	Yes	No	N/A	Yes	N/A	N/A	No	Yes	N/A	Yes

ATTACHMENT B

RFP No. 15: Matrix
Part B: Paper Record Printer System

RFI: Key Information	Populex	Alpha Data Services, Inc.	IVS, LLC	ES&S	TruVote International, Inc.	Bharat Electronics Limited	VeriVote & hp Invent (Partnership)	Vogue Election Systems, LLC	Voting Technologies International	Ferey	Sequoia Voting Systems
Paper Record Printer System	Part of The PopulexSlate base system; no stand alone print system available	Part of the VRES system: Not an add on; no separate purchased required	No stand alone printer syst. that will work w/other systems	Two types: As a stand alone or attached to the iVotronic	No stand alone printer syst. that will work w/other systems	N/A	VeriVote: An independent electronic audit device	N/A	No stand alone printer syst. that will work w/other systems	Real-Time Ballot Printer (RBP): Stand alone unit	No stand alone printer syst. that will work w/other systems
System Availability	N/A	N/A	N/A	Currently testing; not available for sale	N/A	N/A	Currently Available	N/A	N/A	Currently Available	N/A
Does System Interface w/iVotronic	N/A	N/A	N/A	Yes	N/A	N/A	States that this system can be integrated internal or external of a DRE system	N/A	N/A	Not tested with ES&S but states that it is compatible w/iVotronic	N/A
System being used?	N/A	N/A	N/A	For test and developme nt purposes only: Prototype only	N/A	N/A	Did not state	N/A	N/A	With Diebold, AVS, Indra, and Ferey International Being used in Argentina	N/A

ATTACHMENT B

System Certification(s)	N/A	N/A	N/A	None	N/A	N/A	Did not state	N/A	N/A	N/A	N/A
Technical Specs. Provided?	N/A	N/A	N/A	Minimal	N/A	N/A	No	N/A	N/A	Yes	N/A
Estimated Cost(s) Provided?	N/A	N/A	N/A	$800 to $1,200	N/A	N/A	Yes: $155 per unit	N/A	N/A	Yes: Multiple pricing	N/A
Demo Recommended?	N/A	N/A	N/A	Yes	N/A	N/A	Yes	N/A	N/A	Yes	N/A

Touchscreen Voting Systems Issue Paper
Florida State Association of Supervisors of Elections

The 2000 General Election has served as the catalyst for election reform not only in Florida but throughout the United States. In Florida, the most significant reform undertaken was that of requiring the replacement of certain voting systems. Counties were left with the choice of either purchasing an optical scan precinct count system or a direct record electronic (DRE) touchscreen voting system. In the 2002 elections, the new equipment performed exceedingly well in virtually every county which implemented one of these two new systems. The equipment performed well and voters appeared to have little problem utilizing these new systems. In the immediate future, practically every jurisdiction in the country will be moving to the use of one of these systems.

As a result of these reforms, sixteen Florida counties chose to purchase and install touchscreen voting systems. These counties represent over half of all registered voters in Florida. In 2002, the United States Congress passed, and President Bush thereafter signed into law, the Help America Vote Act (HAVA) that requires every county in the United States to provide at least one touchscreen voting booth (DRE) or other voting system that accommodates the blind and/or visually impaired in every polling place no later than January 1, 2006.

With the number of counties that have selected touchscreen systems and the certain increase in use of these systems, some individuals have begun to question their reliability, security and accuracy. Based on these concerns, the Florida Supervisors of Elections feel it is necessary to address these issues to insure our voting public of the integrity of our elections equipment.

Touchscreen voting systems are sophisticated systems, more so than any others previously developed and used. However, because of the simplicity they provide the voter, jurisdictions across our nation are realizing the advantages of these systems. Accuracy and security are two major areas that elections officials find to be central in the selection of systems. Touchscreen systems offer the highest levels of accuracy and security.

Touchscreen systems are designed to capture the voter's choices by touching a screen. The choices are not final until the voter has had the opportunity to verify or change any of his choices. Once the voter is satisfied, the ballot is cast by either touching the screen in an indicated location or by pressing a button located at the top of the voting unit.

All voting systems in use in the State of Florida are approved and certified by the Division of Elections of the Florida Department of State prior to their use. No system can be purchased and thereafter used by any county in the state until this certification takes place.

INDEPENDENT TESTING AUTHORITIES/STATE CERTIFICATION

Prior to any system being certified for use in Florida, the system manufacturer is required to submit it to an independent testing authority (ITA). Independent testing authorities are currently certified by the National Association of State Election Directors' (NASED) ITA Certification Committee. These duties are being transferred to the National Institute of Standards and Testing (NIST) pursuant to HAVA. This transfer of duties is expected to be completed by Fall, 2005. This independent testing authority is INDEPENDENT of any manufacturer, state authority or county elections official. These testing labs (Cyber, Systest, and Wyle) are charged with the responsibility of exposing the hardware to a number of tests. In addition, the software and firmware go through an extensive examination of the source code to ensure that it performs as required by the Federal Election Commission standards...nothing more, nothing less.

Once the ITA completes its review, the system is sent to the State for a complete examination of hardware, firmware and software. Florida's certification process is considered to be one of the most stringent in the nation. The Department of State's Division of Elections, as part of the testing process, conducts an election on each system to verify its performance. If the system is approved and certified, no changes to the system can be made without further examination, testing and certification.

SOURCE CODE/PROPRIETARY SOFTWARE

Much is being said about the lack of availability of the systems' software, firmware and hardware to the general public. Voting systems software is proprietary. Because of this, there is the general thought that it is controlled by the manufacturer, one specific individual or small group of individuals. Nothing could be further from the actual facts. Simply because the software is not open to every hacker in the world, does not mean the software is not reviewed and exposed to public scrutiny.[1] For obvious reasons, strict control of this software is maintained and provides further safeguards from unauthorized individuals altering or tampering for private gain.

Supervisors of elections DO NOT have the source code or any other software or firmware that has the ability to affect the logic of their respective voting systems thereby affecting the tabulation of votes. Source code is required by law to be escrowed with the State as well as escrowed with the independent testing authority. Additionally, NASED requires the manufacturer's software to be escrowed with its written source code. Therefore, this code can always be accessed, by authorized authorities, to insure that it hasn't been improperly changed and is performing in the proper and authorized manner.

OTHER SECURITY ISSUES

Voting systems are very decentralized. There is not one critical nexus that everything must pass in order for an election to be conducted. Because of this decentralization, a

[1] DREs and the Election Process, The Election Center

number of different entities and individuals are involved with the preparation and conduct of the election. As stated above, systems are certified through ITAs and the Division of Elections. After the actual election parameters (office titles, candidates' names, and the number for which voters are allowed to vote) are established at the local county level, the system is required to be publicly tested to insure it is properly programmed, the election is correctly defined and all of the voting system input, output and communication devices are working properly. Candidates and political parties are notified of these tests and the public is given notice as required by law.

Supervisors of elections realize that for voting systems to operate in a secure manner, sound policies and procedures must also be developed that address each component of the process. The actual voting system is just a part of the overall system. The "best" voting system available is only as "secure" as the policies and procedures that govern its use and operation. All interested parties must look beyond the actual system in order to establish its level of security.

It needs to be clearly understood that the touchscreen system, while computerized, is a stand alone system. Each of the voting machines is not tied into any type of integrated database or communication system that would allow it to be tapped into from the outside. Therefore, as we so commonly see with computer systems and communication networks, hacking into these voting machines is not a concern. The process of voting and tabulating the results is not subject to being affected by sources outside the election system process.

VERIFIABLE PAPER RECEIPTS

One of the reasons that counties selected touchscreen voting systems was the elimination of paper. Our society is moving away from requiring paper with much of the business that is being transacted. With this being said, supervisors were very much aware that new systems would have to be able to produce a ballot reproduction, on paper, if ordered to do so for recount purposes and/or by order of a court. HAVA requires the voting system to produce a permanent paper record with a manual audit capacity.[2] Systems must have this capability in order to preserve the reliability and integrity of the system.

A small number of persons has put forth that there be a requirement for touchscreen systems to produce a paper receipt after the voter casts his ballot. The systems currently certified provide the necessary safeguards and security to insure accurate elections. It would appear that the reason this concern arises is either a distrust of technology by the people who would request such a printout or a lack of understanding that in the event that there is a close election or other issue which arises after the election, there is an ability to make a determination of the votes that were actually cast. It may be impossible to eliminate the distrust of modern technology by persons who may have this concern. However, the equipment now in place does provide the elections authorities, as well as the judicial system, a means by which all votes can be ascertained from the images on the DRE system. It is critical to understand that each DRE has a record that can be retrieved

[2] Help America Vote Act, Section 301(a)(2)(B)(i)

from each machine to show the votes that were actually cast by the voter. While it may be a lengthy process, the equipment can provide the authorities with the ability to demonstrate the votes actually cast if a recount or some similar issue presented itself, post election. Therefore, the issue of creating a paper trail for each voter is unnecessary except to eliminate the paranoia of the critics of these systems.

However, there are a number of other concerns beyond merely insuring that there is integrity in the system by being able to recreate the votes that had actually been cast that throw into question the need for a paper receipt. Some of those issues are:

(1) A paper receipt proves nothing. Consider this scenario…a voter selects his candidates on the touchscreen system and votes for "Candidate X." The voter is required to "review" his choices on a review screen before the system will allow the ballot to be cast…the voter's review screen indicates "Candidate X." This review allows the voter to make any changes or corrections to his ballot to prevent the voter from being unclear how he voted. Once the voter is satisfied, he casts his ballot by either touching a determined spot on the screen or pushing a button on the voting unit. Assuming the unit is equipped with a printer, the voter's receipt indicates he voted for "Candidate X." Now that the voter has received his receipt he can then proceed to go to the elections official at the polling place and tell them that he in fact voted for "Candidate Y," yet his receipt shows "Candidate X." Voters who desire to create absolute confusion can throw the election into turmoil if the printed receipt, which is no different than the record which would be maintained on the system, is given substantial impact at this point. The paper receipt therefore proves nothing other than to verify the vote which already is recorded. Punchcard system or lever machine voters did not receive verification of their vote, or that it was in fact counted as cast, other than the trust in the system and process. Likewise, voters using an optical scan system do not receive a receipt and the paper ballot which is retained is identical to the ballot record in the DRE.

(2) Paper receipts violate the spirit and intent of the HAVA which states, "the voting system shall permit the voter to verify (in a private and independent manner) the votes selected by the voter on the ballot before the ballot is cast and counted."[3] Requiring printers would negate the opportunity for blind or visually impaired voters to review "in a private and independent manner" their ballot prior to it being cast. Touchscreen voting systems provide for the very first time the ability for disabled voters to cast a ballot unaided and unassisted. Paper receipts take that opportunity away from these voters. Additionally, the federal requirement of multiple languages on the ballot also presents a challenge that is not contemplated by the proponents of the verifiable paper receipt.

(3) Printers for touchscreen voting booths are not currently available. The systems currently certified are not certified with printers. Requiring printers is not as simple as just plugging a printer into the unit. With printers comes a new set of issues and challenges such as paper jams, running out of ink and paper and the realization that they are a mechanical piece of equipment. Printed receipts for large ballots could be several feet long. Additionally, pollworkers will need to be further trained to connect additional

[3] Help America Vote Act, Section 301(a)(1)(A)(i)

equipment at the polling place on Election Day. Printers add weight to the units complicating precinct setup and increasing the costs for delivery to the polling places.

(4) Counties in Florida that have purchased touchscreen voting systems have invested a great deal of state and local tax dollars. You cannot talk about the paper receipt without discussing the additional cost to local governments to retrofit every touchscreen voting booth with a printer. County governments are cash strapped. Counties that were using punchcard voting systems were, by legislative act, required to abandon these systems for either optical scan or touchscreen systems. These counties have spent millions of dollars to comply with state law. It is estimated that printers would cost an additional $500 to $1,000 each. This is a huge expenditure of funds that counties do not have.

There have been some comments made that counties should use "their portion of HAVA reimbursement" money to purchase these printers. First, it is not clear that HAVA dollars will be available for this purchase. HAVA money set aside for voting systems was set aside for those counties that do not have a DRE system and are being required to purchase at least one device per polling place to allow the disabled voters to cast a ballot unaided and unassisted. Second, it is unclear as to whether or not the HAVA money will "filter down" to the counties. Counties do not have the resources to provide printers for systems that already have a "manual audit capacity" and are already in compliance with federal and state requirements.

(5) Based on our experience, the hand-counting of paper ballots, or in this case receipts, is not as accurate as ballots counted electronically. It should be understood that we are talking about counting, in some instances, many thousands of pieces of paper. The process used to accomplish this task is cumbersome and problematic. Counting teams are human....susceptible to becoming tired, prone to distractions and error. Experience has shown that hand recounts of any paper ballots are not as accurate as when counted on the tabulation system.

(6) Since 1964, electronic voting systems have been used in this nation's elections processes. In almost four decades, not a single case of election fraud due to tampering of a system's hardware or software has occurred. Comparably, in the last 40 years, hundreds of cases of election fraud involving paper have occurred and been successfully prosecuted.[4] The risk exists, depending on the laws, rules, policies and procedures in place, that the use of a paper receipt would open the door for voters to exchange their receipt (their vote) for something of value. Our existing systems do not allow this to happen.

(7) Although mechanical lever machines have been decertified for use in Florida, the argument can be made that lever machines never provided a paper receipt of any kind; yet, voters had a higher degree of comfort with lever machines than any other system.

The call for a verifiable paper receipt is not just being addressed by local elections officials. The Election Center, an international association of voter registration and

[4] American Association of People with Disabilities Policy Statement on Voter Verified Paper Ballots

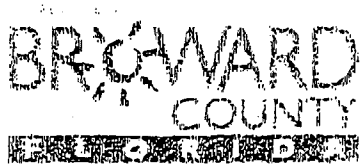
election officials, has written a report addressing the security concerns of DREs which is probably the most comprehensive document to date evaluating these systems. Additionally, The Leadership Conference on Civil Rights, the United States League of Women Voters, and the American Association of People with Disabilities have all produced well written and reasoned papers justifying their positions for not requiring paper receipts.

CONCLUSION

Touchscreen voting systems are like no other type of voting technology used before. These systems are more complex and secure; yet, voters find them very easy to use. These systems have allowed supervisors of elections the opportunity to address many of the critical issues on Election Day such as overvoting, ballot review, and ease of use. Additionally, the greatest advantage these systems provide is the audio ballot allowing blind and visually impaired voters to vote unaided and unassisted for the very first time.

Supervisors of elections realize the apprehension the voting public may experience any time there is a change to new technology. Supervisors and their staffs have worked tirelessly to educate our public about the new systems and the security and reliability they provide. Supervisors are committed to continuing to educate our citizens on how these systems operate as well as being informed about candidates and issues. These groups and individuals who continue to challenge, without justification or proof, the credibility of these systems are committing a huge disservice to the voting public. The continued unfounded attacks on these systems erode the public's confidence. Once the public loses trust in the actual voting system, the elections official, and our elections processes, they have no reason to go to the polls and vote.

ATTACHMENT D



ROGER DESJARLAIS, County Administrator
115 S. Andrews Avenue, Room 409 • Fort Lauderdale, Florida 33301 • 954-357-7350 • FAX 954-357-7360

MEMORANDUM

DATE: November 21, 2003

TO: Ilene Lieberman, Mayor
Kristin Jacobs, Vice-Mayor
& the Board of County Commissioners

FROM: Pete Corwin, Assistant to the County Administrator

SUBJ: Status Report -Voting Systems/Paper Ballots

Throughout the procurement process for a new voting system, the Board stressed the need for a secure voting system and a desire for an auditable paper trail produced by the voter. On September 23rd, the Board discussed the addition of voter verifiable paper ballots or "receipts" to the touch screen voting machines (DRE). The Board directed staff to prepare a report addressing various options and the security of the voting system.

After the November 2000 General Election, the State decertified punchcard voting systems and left Counties with only two choices – an optical scan or touch screen system. In order to comply with the Help America Vote Act (HAVA) and the Americans with Disabilities Act (ADA), all counties will be required to have both an optical scan and DRE system by 2006. The State also enacted election reforms such as provisional ballots, in office voting and no excuse absentee ballots. Recent Federal Legislation (HAVA) adds additional reforms. The decertification of the relatively simple punchcard system and, the other reforms has resulted in a more complicated voting process.

Given the rapid pace of reforms it is not surprising that the perfect voting system does not exist. A "perfect system" should, among other things, be inexpensive to acquire and operate; eliminate over votes and minimize under votes; record votes accurately; produce clear redundant audit trails; permit voters who are visually impaired or have other disabilities to vote independently without assistance; be totally secure from fraud; permit voters to cast their votes anonymously; be flexible to accommodate provisional votes, write in votes and multiple languages; produce a voter verifiable ballot or receipt; produce ballots that clearly indicate voter intent and can be quickly recounted in the case of a close election; be easily upgraded to take advantage of future enhancements; be easy to deploy and store; allow for fast turnarounds between elections; be easy for poll workers to operate and manage; provide fast results that have been verified before being released to the media; etc. No system meets all of these sometimes conflicting objectives.

Broward County Board of County Commissioners
Josephus Eggelletion, Jr. • Ben Graber • Sue Gunzburger • Kristin D. Jacobs • Ilene Lieberman • Lori Nance Parrish • John E. Rodstrom, Jr. • Jim Scott
Diana Wasserman-Rubin
www.broward.org

ATTACHMENT D

This report addresses the security of the ES&S system; voter verifiable paper ballots; options available to the Board; and staff recommendations. To prepare the report staff reviewed available research on these subjects including a recent Congressional Research Service report; a California Task Force report; John Hopkins University report; a Consultant Report produced for the State of Maryland; vendor reports; a conference call and research materials from the Gartner Group; a recent report from the State Supervisors of Elections Association; a report from The Elections Center; position papers from the League of Women Voters, Leadership Conference on Civil Rights and the American Association of People with Disabilities; and numerous articles. In summary, staff has concluded:

- With proper security procedures and controls in place, the ES&S system is secure and can be relied upon to accurately record and tabulate votes.
- A voter produced ballot for DRE's is desirable, but no product is certified and no product (on the market or prototype) appears to provide a cost effective solution.
- This is an evolving issue. Staff will continue to monitor changes in legal requirements, new products and enhancements to security.

SECURITY ISSUES

There is an ongoing national debate regarding the security, reliability and accuracy of DRE systems. Staff has reviewed the available research on the subject and continues to believe that DRE systems in general and ES&S systems in particular are secure, reliable and accurate. According to a recent report by the Florida State Association of Supervisors of Elections (Exhibit "A"), electronic voting systems have been used for 40 years and there has never been a case of election fraud due to tampering with system hardware or software. There have been numerous cases of fraud, but they have occurred due to faulty security procedures, corrupt officials, human error, inaccurate voter rolls and other causes that are potential risks no matter what election system is used to record and tally votes. Any voting system is only as secure and dependable as the procedures that govern the operations of the system and the people who administer the system. Proper procedures and controls with multiple checks and balances are the best protection against voter fraud.

There are a number of misconceptions and misunderstandings that surface in the debate surrounding "computerized" or electronic voting systems. Using computer systems to vote may lead someone to think of several common security risks including computer viruses; hacking through phone lines; hacking through the internet; network vulnerability; and software design flaws or "bugs". Neither the voting machines nor the tabulation system (Unity) are connected to a network or the internet, therefore, there is no risk of hacking. The voting machines are not connected to phone lines. Only preliminary results are transmitted via modem to the tabulation system and they are encrypted. Elections software used in Florida undergoes numerous rounds of testing to uncover and fix design flaws or "bugs". Every line of code is inspected by an independent testing authority before the State begins their vigorous certification process. Some have raised the concern that a corrupt programmer working for a vendor could corrupt a program and influence the outcome of an election. Staff does not believe it is feasible for a single person working for a vendor or the SOE to modify election

Broward County Board of County Commissioners
Josephus Eggelletion, Jr. • Ben Graber • Sue Gunzburger • Kristin D. Jacobs • Ilene Lieberman • Lori Nance Parrish • John E. Rodstrom, Jr. • Jim Scott
Diana Wasserman-Rubin
www.broward.org

results without being detected. The Gartner Group believes DRE systems are more secure or at a minimum, as secure as other voting systems. They also believe to successfully alter results, requires collusion on the part of multiple parties and this potential risk exists in all systems and can be mitigated with proper security procedures and controls. Exhibit "B" addresses a list of common misconceptions in more detail.

Staff reviewed recent reports that addressed the security of DRE systems and compared the findings in those reports with the ES&S system used in Broward County. The first is a report by John Hopkins University computer scientists who analyzed the Diebold system and identified 12 areas in which the system was vulnerable to attack. Exhibit "C" lists each of the 12 areas and how these issues are either irrelevant to the ES&S system or have been mitigated.

Staff also reviewed a report prepared by a consultant for the State of Maryland in response to the John Hopkins report. The consultant performed a risk assessment of the Diebold system and the State's procedures and controls. They recommended 17 mitigation strategies to address high risk areas. Only three are technical issues and 14 are procedural issues. Exhibit "D" lists each of the 17 recommendations and how these issues are either irrelevant to the ES&S system or have been mitigated.

In conclusion, staff believes the ES&S system is secure, reliable and accurate. There are numerous controls and safeguards in place including:

- Independent testing labs that test all DRE systems based upon national elections standards.
- State Division of Elections testing and certification based upon very stringent state standards for all new systems and all modifications/upgrades.
- Source code held in escrow by the State Division of Elections.
- Public Logic & Accuracy tests before the Canvassing Board, candidates and the general public/media.
- "Clear and test" operations performed prior to use on election day to insure all machines and PEB's start the voting at zero.
- Multiple audit files (redundancy) in each machine to protect against "lost" votes. Votes cannot be recorded unless all files are operational and capable of recording votes.
- Each election has unique codes and passwords.
- Audit logs capture every event to insure that if anyone tampers with a machine it is detected and does not go unnoticed
- Operation and Security Plan from the SOE on file with the State Division of Elections.

Attached (Exhibit E) is a report issued by ES&S that provides additional details.

As stated above, security procedures and controls are the most important aspect of any voting system and they should be continually reevaluated and strengthened. Staff recommends studying the feasibility of enhancements such as a bar-coding system to track all machines, PEB's and the people who handle them (i.e. a chain of custody); enhanced L&A tests to provide an even greater degree of confidence in the system; review and performance audit of the SOE security plan to assess potential risks and strengthen procedures if necessary; and

Broward County Board of County Commissioners
Josephus Eggelletion, Jr. • Ben Graber • Sue Gunzburger • Kristin D. Jacobs • Ilene Lieberman • Lori Nance Parrish • John E. Rodstrom, Jr. • Jim Scott
Diana Wasserman-Rubin
www.broward.org

enhanced post election tests such as comparing the number of voters who signed in to vote with the number of ballots cast and verifying certified vote totals to the vote totals from the audit files.

Enhancing security is an ongoing process and elections officials are continuously working to insure the integrity of the voting process. DRE systems are new and as best practices are deployed in other jurisdictions they should be considered for implementation.

VOTER VERIFIABLE PAPER BALLOTS

Staff believes that the issue of producing a paper ballot created by voters, is separate from insuring that the voting system is secure. As discussed above, if adequate security procedures and controls are in place, the ES&S system is secure and will count votes accurately. Several organizations (such as the League of Women Voters and the American Association of People with Disabilities) have issued position papers opposing adding a paper ballot to DRE machines. Some voters, however, want to see and/or touch a paper ballot that they have produced in order to have confidence that their vote is recorded accurately. The voter sees their review screen, but does not see the electronic image that records their vote inside the machine and may not trust the machine to do this accurately. While the vote is recorded in three redundant audit files and a ballot image can be printed out in case of an audit or court challenge, critics maintain that the machine produced the redundant images not the voter. In addition, many policy makers believe that it is important to have a voter produced paper ballot that can be used in a recount to verify results. They argue that if a recount is required only paper ballots produced by the voter should be used to determine the winner. These potential enhancements to the ES&S system are policy issues to be determined by the Board.

Some people believe that HAVA requires a voter produced paper receipt. The County Attorney does not concur. State Statutes require DRE machines to maintain a random sorted file of ballot images for every vote cast - not produce a paper ballot for the voter. The ES&S machines have a serial port that can accommodate a printer that can produce ballot records if needed for an audit or court challenge. There is, however, legislation pending in Congress that would mandate paper ballots.

The ES&S system currently produces a paper audit trail, but it does not reproduce each voter's ballot in case of a recount. At the end of the voting day, each precinct's Master PEB is used to produce a paper log which shows the votes for each race by machine and tallies the results for all races in that precinct. Before the results are certified, the paper log is compared to the results that are sent from the Master PEB to the Tabulation system via modem. If a recount is required, Supervisor of Election staff rerun and retally all of the votes from all of the Master PEB's. If necessary, results can be obtained from each individual machine by downloading the audit files directly into the tabulation system. The system does not produce paper ballots to be used for a recount, however, a ballot record of each vote cast can be printed out if necessary for audit purposes. None of the three DRE systems certified for use in the State create paper ballots for each vote cast and there are no printers ready to be certified by the State Division of Elections.

Broward County Board of County Commissioners
Josephus Eggelletion, Jr. • Ben Graber • Sue Gunzburger • Kristin D. Jacobs • Ilene Lieberman • Lori Nance Parrish • John E. Rodstrom, Jr. • Jim Scott
Diana Wasserman-Rubin
www.broward.org

ATTACHMENT D

There are several ways vendors may develop products to create a voter produced paper trail including:

- A paper ballot inside the machine to be used in case of a recount, the voter does not see it or touch it.
- A paper receipt "Under glass" – the voter sees it but does not touch it. The voter could compare the paper ballot to the review screen prior to hitting the "Vote" button, but does not take it to a separate ballot box.
- A paper ballot produced by an external printer which the voter places in a ballot box to be used in case of a recount.
- A paper "receipt" produced by an external printer which the voter retains

At this point in time, no product has been developed that overcomes the inherent disadvantages of a paper voting system. The introduction of paper into the voting process creates a number of challenges:

- Printers jam, run out of paper, and run out of ink.
- Printers must be deployed, set up, maintained and stored.
- Voters may forget to place their ballots in the box or argue that their paper ballot is different then what was on the review screen.
- Voters will take longer to vote if they compare the review screen to a printed ballot which may result in longer lines or more machines.
- If a voter changes their mind the paper ballot produced by the machine must be destroyed. Control of spoiled ballots is a concern and could raise doubts about the integrity of the process.
- Paper ballots are open to interpretation of voter intent and will take much longer to count.
- Visually impaired voters cannot verify a paper ballot without assistance.

All of these challenges can be overcome with sound management practices, increased staffing and advances in DRE technology and products.

ES&S has developed a prototype printer so that a voter can see their ballot (under Plexiglas) and change their choices. It is not in production and has not been certified. The ES&S prototype may cost between $500 to $1,000 each or from $3 to $6 million total. If voters take longer to vote as a result of the printers, additional iVotronics may be required. There would also be additional costs to maintain and store the printers plus operating supplies (paper and ribbons) and training costs. Some have suggested using HAVA funds for this purpose, however, the vast majority of HAVA funds allocated to Florida will be retained by the State. Staff believes the only HAVA funds Florida counties can expect to receive will be for voter education.

Staff recommends that the Board wait for vendors to develop a cost effective method for a voter produced ballot. It may not be paper. Vendors may be able to produce an image of a ballot that is stored in the machine and machine readable by a scanner or other device. MIT Media Labs is reportedly working on a system with multiple verifiable programs. Vendors such

Broward County Board of County Commissioners
Josephus Eggelletton, Jr. • Ben Graber • Sue Gunzburger • Kristin D. Jacobs • Ilene Lieberman • Lori Nance Parrish • John E. Rodstrom, Jr. • Jim Scott
Diana Wasserman-Rubin
www.broward.org

as VoteHere have software products for DRE machines that may allow each voter to verify their vote. Staff believes that if there is a market, vendors will develop products that meet the need. The solution will need to be tested and certified and staff recommends that the Board also wait until any new product is field tested in actual elections prior to purchase.

OPTICAL SCAN

One option that the Board briefly discussed was to switch from a DRE to an optical scan system. Staff does not recommend converting to an optical scan system. Aside from the capital costs of approximately $4.3 million to acquire optical readers for each precinct, the operating costs for an optical system would be significantly higher as compared to a DRE system. Some costs such as temporary workers to prepare the iVotronics and transportation may decrease, however, increased printing costs would more than make up for any savings. ES&S charges $.25 to print a one page ballot. A three page ballot for a general election would cost approximately $750,000 to print. Aside from cost, voters tend to favor touch screen systems and find them easy to use. It is also important to remember that we must continue to operate a DRE system to comply with HAVA.

CONCLUSION

Staff believes that the ES&S voting system is secure and can be relied upon to accurately record and tabulate results. Security procedures and controls, however, should be continually reevaluated and strengthened. The Board does not currently have the option to purchase printers in order to provide a voter produced paper ballot or receipt. Staff does not anticipate that a printer will be certified in time for the 2004 elections. Research is ongoing to meet the need for a voter verifiable ballot and the solution may not be a paper ballot. Assuming a printer or other product is certified, staff recommends waiting for other jurisdictions to test it in actual elections.

As the Board considers these issues, it is important to remember that we are in the middle of a national debate and staff does not anticipate a quick or decisive resolution. Congress may pass legislation requiring paper ballots; the Elections Assistance Committee established under HAVA will assume responsibility for testing new voting software and hardware and is likely to establish new rules; the National Institute of Standards and Technology will take a lead role in developing new standards for voting system certification; court rulings regarding ADA requirements may force change; research labs such as MIT will design improvements; vendors will develop new products; and jurisdictions will test the feasibility of new products in actual elections. Staff will continue to monitor these developments and keep the Board informed.

PC/eal/ca

cc: Brenda Snipes, Supervisor of Elections
Roger Desjarlais, County Administrator
Bertha Henry, Deputy County Administrator
Ed Dion, County Attorney
Evan Lukic, County Auditor
Kayla Olsen, Office of Budget Services

Broward County Board of County Commissioners
Josephus Eggelletion, Jr. • Ben Graber • Sue Gunzburger • Kristin D. Jacobs • Ilene Lieberman • Lori Nance Parrish • John E. Rodstrom, Jr. • Jim Scott
Diana Wasserman-Rubin
www.broward.org

Exhibit A ATTACHMENT D

Touchscreen Voting Systems Issue Paper
Florida State Association of Supervisors of Elections

The 2000 General Election has served as the catalyst for election reform not only in Florida but throughout the United States. In Florida, the most significant reform undertaken was that of requiring the replacement of certain voting systems. Counties were left with the choice of either purchasing an optical scan precinct count system or a direct record electronic (DRE) touchscreen voting system. In the 2002 elections, the new equipment performed exceedingly well in virtually every county which implemented one of these two new systems. The equipment performed well and voters appeared to have little problem utilizing these new systems. In the immediate future, practically every jurisdiction in the country will be moving to the use of one of these systems.

As a result of these reforms, sixteen Florida counties chose to purchase and install touchscreen voting systems. These counties represent over half of all registered voters in Florida. In 2002, the United States Congress passed, and President Bush thereafter signed into law, the Help America Vote Act (HAVA) that requires every county in the United States to provide at least one touchscreen voting booth (DRE) or other voting system that accommodates the blind and/or visually impaired in every polling place no later than January 1, 2006.

With the number of counties that have selected touchscreen systems and the certain increase in use of these systems, some individuals have begun to question their reliability, security and accuracy. Based on these concerns, the Florida Supervisors of Elections feel it is necessary to address these issues to insure our voting public of the integrity of our elections equipment.

Touchscreen voting systems are sophisticated systems, more so than any others previously developed and used. However, because of the simplicity they provide the voter, jurisdictions across our nation are realizing the advantages of these systems. Accuracy and security are two major areas that elections officials find to be central in the selection of systems. Touchscreen systems offer the highest levels of accuracy and security.

Touchscreen systems are designed to capture the voter's choices by touching a screen. The choices are not final until the voter has had the opportunity to verify or change any of his choices. Once the voter is satisfied, the ballot is cast by either touching the screen in an indicated location or by pressing a button located at the top of the voting unit.

All voting systems in use in the State of Florida are approved and certified by the Division of Elections of the Florida Department of State prior to their use. No system can be purchased and thereafter used by any county in the state until this certification takes place.

ATTACHMENT D

INDEPENDENT TESTING AUTHORITIES/STATE CERTIFICATION

Prior to any system being certified for use in Florida, the system manufacturer is required to submit it to an independent testing authority (ITA). Independent testing authorities are currently certified by the National Association of State Election Directors' (NASED) ITA Certification Committee. These duties are being transferred to the National Institute of Standards and Testing (NIST) pursuant to HAVA. This transfer of duties is expected to be completed by Fall, 2005. This independent testing authority is INDEPENDENT of any manufacturer, state authority or county elections official. These testing labs (Cyber, Systest, and Wyle) are charged with the responsibility of exposing the hardware to a number of tests. In addition, the software and firmware go through an extensive examination of the source code to ensure that it performs as required by the Federal Election Commission standards...nothing more, nothing less.

Once the ITA completes its review, the system is sent to the State for a complete examination of hardware, firmware and software. Florida's certification process is considered to be one of the most stringent in the nation. The Department of State's Division of Elections, as part of the testing process, conducts an election on each system to verify its performance. If the system is approved and certified, no changes to the system can be made without further examination, testing and certification.

SOURCE CODE/PROPRIETARY SOFTWARE

Much is being said about the lack of availability of the systems' software, firmware and hardware to the general public. Voting systems software is proprietary. Because of this, there is the general thought that it is controlled by the manufacturer, one specific individual or small group of individuals. Nothing could be further from the actual facts. Simply because the software is not open to every hacker in the world, does not mean the software is not reviewed and exposed to public scrutiny.[1] For obvious reasons, strict control of this software is maintained and provides further safeguards from unauthorized individuals altering or tampering for private gain.

Supervisors of elections DO NOT have the source code or any other software or firmware that has the ability to affect the logic of their respective voting systems thereby affecting the tabulation of votes. Source code is required by law to be escrowed with the State as well as escrowed with the independent testing authority. Additionally, NASED requires the manufacturer's software to be escrowed with its written source code. Therefore, this code can always be accessed, by authorized authorities, to insure that it hasn't been improperly changed and is performing in the proper and authorized manner.

OTHER SECURITY ISSUES

Voting systems are very decentralized. There is not one critical nexus that everything must pass in order for an election to be conducted. Because of this decentralization, a

[1] DREs and the Election Process, The Election Center

number of different entities and individuals are involved with the preparation and conduct of the election. As stated above, systems are certified through ITAs and the Division of Elections. After the actual election parameters (office titles, candidates' names, and the number for which voters are allowed to vote) are established at the local county level, the system is required to be publicly tested to insure it is properly programmed, the election is correctly defined and all of the voting system input, output and communication devices are working properly. Candidates and political parties are notified of these tests and the public is given notice as required by law.

Supervisors of elections realize that for voting systems to operate in a secure manner, sound policies and procedures must also be developed that address each component of the process. The actual voting system is just a part of the overall system. The "best" voting system available is only as "secure" as the policies and procedures that govern its use and operation. All interested parties must look beyond the actual system in order to establish its level of security.

It needs to be clearly understood that the touchscreen system, while computerized, is a stand alone system. Each of the voting machines is not tied into any type of integrated database or communication system that would allow it to be tapped into from the outside. Therefore, as we so commonly see with computer systems and communication networks, hacking into these voting machines is not a concern. The process of voting and tabulating the results is not subject to being affected by sources outside the election system process.

VERIFIABLE PAPER RECEIPTS

One of the reasons that counties selected touchscreen voting systems was the elimination of paper. Our society is moving away from requiring paper with much of the business that is being transacted. With this being said, supervisors were very much aware that new systems would have to be able to produce a ballot reproduction, on paper, if ordered to do so for recount purposes and/or by order of a court. HAVA requires the voting system to produce a permanent paper record with a manual audit capacity.[2] Systems must have this capability in order to preserve the reliability and integrity of the system.

A small number of persons has put forth that there be a requirement for touchscreen systems to produce a paper receipt after the voter casts his ballot. The systems currently certified provide the necessary safeguards and security to insure accurate elections. It would appear that the reason this concern arises is either a distrust of technology by the people who would request such a printout or a lack of understanding that in the event that there is a close election or other issue which arises after the election, there is an ability to make a determination of the votes that were actually cast. It may be impossible to eliminate the distrust of modern technology by persons who may have this concern. However, the equipment now in place does provide the elections authorities, as well as the judicial system, a means by which all votes can be ascertained from the images on the DRE system. It is critical to understand that each DRE has a record that can be retrieved

[2] Help America Vote Act, Section 301(a)(2)(B)(i)

ATTACHMENT D

from each machine to show the votes that were actually cast by the voter. While it may be a lengthy process, the equipment can provide the authorities with the ability to demonstrate the votes actually cast if a recount or some similar issue presented itself, post election. Therefore, the issue of creating a paper trail for each voter is unnecessary except to eliminate the paranoia of the critics of these systems.

However, there are a number of other concerns beyond merely insuring that there is integrity in the system by being able to recreate the votes that had actually been cast that throw into question the need for a paper receipt. Some of those issues are:

(1) A paper receipt proves nothing. Consider this scenario...a voter selects his candidates on the touchscreen system and votes for "Candidate X." The voter is required to "review" his choices on a review screen before the system will allow the ballot to be cast...the voter's review screen indicates "Candidate X." This review allows the voter to make any changes or corrections to his ballot to prevent the voter from being unclear how he voted. Once the voter is satisfied, he casts his ballot by either touching a determined spot on the screen or pushing a button on the voting unit. Assuming the unit is equipped with a printer, the voter's receipt indicates he voted for "Candidate X." Now that the voter has received his receipt he can then proceed to go to the elections official at the polling place and tell them that he in fact voted for "Candidate Y," yet his receipt shows "Candidate X." Voters who desire to create absolute confusion can throw the election into turmoil if the printed receipt, which is no different than the record which would be maintained on the system, is given substantial impact at this point. The paper receipt therefore proves nothing other than to verify the vote which already is recorded. Punchcard system or lever machine voters did not receive verification of their vote, or that it was in fact counted as cast, other than the trust in the system and process. Likewise, voters using an optical scan system do not receive a receipt and the paper ballot which is retained is identical to the ballot record in the DRE.

(2) Paper receipts violate the spirit and intent of the HAVA which states, "the voting system shall permit the voter to verify (in a private and independent manner) the votes selected by the voter on the ballot before the ballot is cast and counted."[3] Requiring printers would negate the opportunity for blind or visually impaired voters to review "in a private and independent manner" their ballot prior to it being cast. Touchscreen voting systems provide for the very first time the ability for disabled voters to cast a ballot unaided and unassisted. Paper receipts take that opportunity away from these voters. Additionally, the federal requirement of multiple languages on the ballot also presents a challenge that is not contemplated by the proponents of the verifiable paper receipt.

(3) Printers for touchscreen voting booths are not currently available. The systems currently certified are not certified with printers. Requiring printers is not as simple as just plugging a printer into the unit. With printers comes a new set of issues and challenges such as paper jams, running out of ink and paper and the realization that they are a mechanical piece of equipment. Printed receipts for large ballots could be several feet long. Additionally, pollworkers will need to be further trained to connect additional

[3] Help America Vote Act, Section 301(a)(1)(A)(i)

ATTACHMENT D

equipment at the polling place on Election Day. Printers add weight to the units complicating precinct setup and increasing the costs for delivery to the polling places.

(4) Counties in Florida that have purchased touchscreen voting systems have invested a great deal of state and local tax dollars. You cannot talk about the paper receipt without discussing the additional cost to local governments to retrofit every touchscreen voting booth with a printer. County governments are cash strapped. Counties that were using punchcard voting systems were, by legislative act, required to abandon these systems for either optical scan or touchscreen systems. These counties have spent millions of dollars to comply with state law. It is estimated that printers would cost an additional $500 to $1,000 each. This is a huge expenditure of funds that counties do not have.

There have been some comments made that counties should use "their portion of HAVA reimbursement" money to purchase these printers. First, it is not clear that HAVA dollars will be available for this purchase. HAVA money set aside for voting systems was set aside for those counties that do not have a DRE system and are being required to purchase at least one device per polling place to allow the disabled voters to cast a ballot unaided and unassisted. Second, it is unclear as to whether or not the HAVA money will "filter down" to the counties. Counties do not have the resources to provide printers for systems that already have a "manual audit capacity" and are already in compliance with federal and state requirements.

(5) Based on our experience, the hand-counting of paper ballots, or in this case receipts, is not as accurate as ballots counted electronically. It should be understood that we are talking about counting, in some instances, many thousands of pieces of paper. The process used to accomplish this task is cumbersome and problematic. Counting teams are human....susceptible to becoming tired, prone to distractions and error. Experience has shown that hand recounts of any paper ballots are not as accurate as when counted on the tabulation system.

(6) Since 1964, electronic voting systems have been used in this nation's elections processes. In almost four decades, not a single case of election fraud due to tampering of a system's hardware or software has occurred. Comparably, in the last 40 years, hundreds of cases of election fraud involving paper have occurred and been successfully prosecuted.[4] The risk exists, depending on the laws, rules, policies and procedures in place, that the use of a paper receipt would open the door for voters to exchange their receipt (their vote) for something of value. Our existing systems do not allow this to happen.

(7) Although mechanical lever machines have been decertified for use in Florida, the argument can be made that lever machines never provided a paper receipt of any kind; yet, voters had a higher degree of comfort with lever machines than any other system.

The call for a verifiable paper receipt is not just being addressed by local elections officials. The Election Center, an international association of voter registration and

[4] American Association of People with Disabilities Policy Statement on Voter Verified Paper Ballots

election officials, has written a report addressing the security concerns of DREs which is probably the most comprehensive document to date evaluating these systems. Additionally, The Leadership Conference on Civil Rights, the United States League of Women Voters, and the American Association of People with Disabilities have all produced well written and reasoned papers justifying their positions for not requiring paper receipts.

CONCLUSION

Touchscreen voting systems are like no other type of voting technology used before. These systems are more complex and secure; yet, voters find them very easy to use. These systems have allowed supervisors of elections the opportunity to address many of the critical issues on Election Day such as overvoting, ballot review, and ease of use. Additionally, the greatest advantage these systems provide is the audio ballot allowing blind and visually impaired voters to vote unaided and unassisted for the very first time.

Supervisors of elections realize the apprehension the voting public may experience any time there is a change to new technology. Supervisors and their staffs have worked tirelessly to educate our public about the new systems and the security and reliability they provide. Supervisors are committed to continuing to educate our citizens on how these systems operate as well as being informed about candidates and issues. These groups and individuals who continue to challenge, without justification or proof, the credibility of these systems are committing a huge disservice to the voting public. The continued unfounded attacks on these systems erode the public's confidence. Once the public loses trust in the actual voting system, the elections official, and our elections processes, they have no reason to go to the polls and vote.

ATTACHMENT D

EXHIBIT B
COMMON MISCONCEPTIONS

Misconception	Comment
The DRE devices can have their software tampered with to alter resulting vote counts.	The ES&S DRE devices do not contain software which can be altered. The devices contain firmware identified by release number, passwords, cyclic redundancy algorithm checks, and certified by Federal and State agencies. Installation of new, which includes changes to existing, firmware can only be accomplished through a proprietary upload mechanism not commercially available in the marketplace. The devices are basically counters which count ballot positions defined by the UNITY software and transferred to the DRE via the PEB.
Software could be tampered with on the UNITY network to alter resulting vote counts.	This is very unlikely in a secured PC/LAN environment. The Unity security audit logs contain any and every event or action performed on the database, so any attempt would be detected. Unity vote counts are stored in a proprietary, binary format indecipherable outside the Unity software. Additionally, the Unity and iVotronic canvassing procedures, which allow official results to be re-accumulated from the original PEBs iVotronic, would override any procedural errors or changes that might have occurred in the vote counts.
Ballots or vote results could be tampered with by hackers.	Hacking requires the hacker to gain access to the computer or network. This happens in one of two ways; hands on access to the computer, or gaining access via a modem connection either over the internet or by dialing into the modem with the modems phone number. The DRE devices themselves are never connected to a modem thus never connected to the internet, I.E. impossible to hack. The UNITY network is in a secure location protected by a combination locked door. The UNITY network is password protected requiring User ID's to access. The UNITY network is not internet connected. The UNITY network does contain modems for transferring preliminary vote results. However, the modems are connected and communicate with specialized software utilizing a proprietary transmission protocol including an authentication process requiring the incoming caller be recognized or the transmission is terminated. The modems are not left powered on and once the preliminary results are received they are disconnected.

ATTACHMENT D

The DRE devices or the UNITY network is subject to virus attacks.	No part of the election system ever touches the internet reducing the probably of virus attacks. The DRE devices themselves contain no software and the UNITY network is virus protected to prevent infections. Regular backups of the UNITY network take place. Original copies of the certified software are always on hand if a rebuild is necessary. Prior election results are also available from special backups and from the PEBs or the DRE memory devices until erased in preparation for a new election.
Vote results transferred via modem could be intercepted and altered.	To prevent file corruption during electronic transmission of voting results, ES&S utilizes log in passwords to prevent tampering. During transmission of results, which utilize a proprietary protocol, if any file corruption is detected, that file transmission is interrupted and rejected. Additionally, the results transferred are later verified against the opening and closing tapes directly from the precincts, which includes votes by race.

ATTACHMENT D

EXHIBIT C
JOHN HOPKINS UNIVERSITY FINDINGS AND COMMENTS

John Hopkins comment	Broward's implementation
Vote multiple times using forged smartcard.	The ES&S equipment utilizes PEBs and does not utilize smartcards. The voter never handles the PEB, the Poll Worker handles the PEB.
Access administrative functions or close polling station.	The Clerk can physically close the polling location as well as close the voting terminals. This can happen regardless of the voting technology being employed. Poll worker procedures should cover this potential event.
Modify screen configuration.	The screen configurations, ballots, are loaded into the voting devices via the PEB and not modifiable on the device itself. The PEBs can only be modified by a Supervisor terminal (hardware device) located at the central site on the UNITY network.
Impersonate legitimate voting machine to tallying authority.	All iVotronic DRE devices are prepared for an election with an Election Qualification Code. Before each vote is recorded the PEB initiates the ballot and also communicates with the DRE the correct EQC code. Audit logs are maintained to track the DRE devices, which bar codes were delivered to each precinct and which bar codes were returned. The Opening and closing tapes in addition to the ballot activity also contain the specific DRE Serial Number of each DRE device opened and closed. These tapes are audited to verify vote counts recorded in Unity.
Modify ballot definitions (e.g., party affiliation).	Not possible for Poll Workers. If this were done by a systems person creating the master ballot images it would be identified in the ballot review as well as in the L&A testing. Unity would also log the change in the audit log. If changes to the election definitions occurred after burning the PEBs, a date-time database mismatch error message at the time of vote collection would present itself.
Cause votes to be miscounted by tampering with configuration.	The ability to make last minute modifications by systems staff to ballots is necessary to accommodate last minute changes in election requirements which may enable tampering with the configuration. However this should be controlled procedurally.
Tamper with audit logs.	Not possible for Poll Workers. Tampering with audit logs by a systems person would serve little to no purpose. Votes are recorded on election night prior to anyone having sufficient time to gain unobserved access to the logs. The logs are not used to count votes but identify actions taken on the DRE devices.
Create, delete, and modify votes on device.	Impossible to modify votes. Creating or deleting votes would require a poll worker perform supervisory actions on the DRE device also causing a discrepancy between the voter sign in registers and the DRE results.
Link votes to voters.	This is not possible with votes on the DRE devices. This could be possible with the use of hard copy provisional or absentee ballots.
Delay the start of an election.	Possible regardless of the voting devices being utilized.
Tamper with election results.	Since items 1 through 10 identified specific attacks this is either a summary or indicating the tampering on the master tally computer. Since all votes whether punched card, optical, or DRE are counted by computers this scenario is possible regardless of the voting devices being utilized.
Insert backdoors into code.	Correctness of the software is proven through extensive testing processes by the vendor, independent testing authorities, both Federal and state certification processes, and at the jurisdiction during the Logic and Accuracy testing. Every single line of code is inspected by the FEC Independent Testing Authority (ITA) for any type of malicious or mischievous code. Electronic voting, in many ways, is a much more reliable, accurate and secure system.

ATTACHMENT D

EXHIBIT D
MARYLAND CONSULTANTS' RECOMENDATIONS

Maryland issues – Technical	Comment on Broward's implementation
Apply cryptographic protocols to protect transmission of vote tallies.	To prevent file corruption during electronic transmission of voting results, ES&S utilizes log-in passwords to prevent tampering. During transmission of results, which encrypts the data and employs proprietary protocols, if any file corruption is detected, that file transmission is interrupted and rejected.
Remove the SBE GEMS server immediately from any network connections. Rebuild the server from trusted media to assure and validate that the system has not been compromised. Remove all extraneous software not required for AccuVote-TS operation. Move the server to a secure location.	The SOE UNITY network is and always was stand alone. It is not connected to the Internet, contains no extraneous software. The physical location of system components is within a secure area protected by combination lock, with limited controlled access.
Discontinue the use of an FTP server to distribute the approved ballots.	FTP was never utilized for ballot distribution.
Maryland issues - Procedural	
Bring the AccuVote-TS voting system into compliance with the State of Maryland Information Security Policy and Standards.	The Broward SOE Unity network is Florida State certified and vendor installed.
Consider the creation of a Chief Information Systems Security Officer (CISSO) position at SBE. This individual would be responsible for the secure operations of the AccuVote-TS voting system.	The State Division of Elections reviews security issues. If the SOE does not already have a person designated to review and monitor security policies one should be identified. These policies would cover the IT procedures as well as all the manual operational procedures.
Develop a formal, documented, complete, and integrated set of standards policies and procedures. Apply these standard policies and procedures consistently through the Local Board of Elections (LBEs) in all jurisdictions.	The Broward SOE must submit a plan to the Florida Elections Commission covering formal standard policies and procedures in regards to security.
Create a formal, System Security Plan. The plan should be consistent with the State of Maryland Information Security Policy and Standards, Code of Maryland Regulations (COMAR), Federal Election Commission (FEC) standards, and industry best practices.	The Broward SOE must submit a plan to the Florida Elections Commission covering standard policies and procedures in regards to security.
Require 100 percent verification of results transmitted to the media through separate	Procedures include the review of the poll opening and closing tapes and the comparison of those vote totals to

ATTACHMENT D

count of PCMCIA cards containing the original votes cast.	those recorded by the vote transmissions.
Establish a formal process requiring the review of audit trails at both the application and operating system levels.	These processes should be included in the document required by the Florida Elections Commission.
Provide formal information security awareness, training, and education program appropriate to each user's level of access.	This training requirement should be addressed by Broward's SOE.
Review any system modifications through formal, documented, risk assessment process to ensure that changes do not negate existing security controls. Perform a formal risk assessment following any major system modifications, or at least every three years.	The Florida Elections Commission certifies all system modifications made by the vendor which includes vigorous testing. The Broward SOE's Security policy should also address the testing of any new environment changes. In regards to formal risk assessments taking place every three years regardless of modifications, risk assessment should be an on-going event with the policies in a continual process of refinement.
Implement a formal, documented process to detect and respond to unauthorized transaction attempts by authorized and / or unauthorized users.	This should be an included component of the Broward SOE Security policy.
Establish a formal, documented set of procedures describing how the general support system identifies access to the system.	This should be an included component of the Broward SOE Security policy.
Change default passwords and passwords printed in documentation immediately.	If these cases are present at the Broward SOE they also should be addressed immediately.
Verify through established procedures that the ITA- certified version of software and firmware is loaded prior to product implementation.	This should be an included component of the Broward SOE Security plan. This procedure has been in place and is taking place while preparing the DRE devices for an upcoming election.
Modify procedures for the Logic and Accuracy (L&A) testing to include testing of time oriented exploits (e.g. Trojans).	This could be an included component of Broward's L&A testing.
Implement an iterative process to ensure that the integrity of the AccuVote-TS voting system is maintained throughout the lifecycle process.	All changes made to the voting hardware and software are certified by the Florida Elections Commission prior to arriving here at the Broward SOE.

Exhibit E ATTACHMENT D

White Paper: "Protecting the Integrity of America's Elections – Tamper Detection and Prevention in Voting Equipment"

Background

In the past decade technology has provided tremendous strides in the way ballots are cast and counted. New generations of computerized voting equipment and software have improved the election tabulation, accumulation and report generation process. Most importantly, modern voting equipment is accurate, efficient, reliable and verifiable.

There are three types of computerized voting equipment at present:

- Punch Cards – Voters cast votes by punching holes with a stylus in a response area on a computer punch card. The cards are collected and tabulated at a central location after the polls close. This system has been the mainstay of computerized voting for many decades although events surrounding the 2000 elections have tarnished its value. While several states have banned punch card voting, many others still use this system.
- Optical Scan/Optical Mark Reader (OMR) – OMR equipment can be used in centrally located counting centers after ballots are collected, or they can be individual precinct based. To vote, a voter marks a preprinted paper ballot with a specified marking device. OMR systems record the votes by scanning or "detecting" marks made on the ballots.
- Direct Recording Electronic (DRE) – DRE voting systems are precinct based electronic iteration of the traditional lever voting machine. To vote, voters enter choices directly into the DRE system memory through a touch screen or keypad as the ballot image appear. DRE systems do not use paper ballots but votes are stored in memory for collection after the polls close.

With the advent of and significant increase in usage of electronic voting since the 2000 elections, a better understanding of the safeguards and procedures currently in place to prevent and detect tampering of OMR and DRE equipment is necessary to engender public trust.

Skeptics abound when computerized, and in particular, paperless voting is mentioned. Detractors who have not examined the issue closely concoct a theory of conspiracy by devious corporations and manipulation of votes.

In reality, computerized voting, in particular OMR and DRE voting in its present form is ***easy***, ***safe*** and ***secure***. There are many safeguards, checks and balances built into the process involving procurement, certification, pre-testing,

Copyright August, 2002

audit reports and results verification. Ultimately, there is a chain of accountability in the current system. Computer voting today should be no different than using airline, banking or telecommunication services.

The focus of this paper will be on current best practices as they relate to election equipment tamper prevention and detection procedures in general. Issues related to election improvements such as Internet voting or voter registration are not included here but available in a separate ES&S Internet Voting White Paper.

Election Security and Fraud

Before describing existing safeguards and practices, it is useful to distinguish between fraud and tampering.

There are two types of possible fraud in any election: 1) campaign finance and ethics-related fraud, and 2) election-related fraud. Federal fraud prevention statutes have existed since the Enforcement Acts of 1866. Current fraud laws are powerful and diligently enforced by the Justice Department.

Fraud can be committed in one of two major ways: 1) compromising the voter registration system (such as breaching provisions provided for under the National Voter Registration Act), or 2) compromising the election system. Computerized voting equipment tampering would fall into the latter category.

There are two main types of election security concerns related to tampering:

1. Disruption of the Election Process: This includes interruption of the voting and/or vote counting process. Protecting a voting system from process disruption is accomplished by controlling physical access to the system.
2. Corruption of Ballot Data: Ballot data is protected from tampering with advanced database management, encryption and authentication techniques that guarantee data integrity. Access control is also important.

It should be noted that despite periodic allegation of "vote fixing" and "equipment tampering" in the news, to date, there has not been solid evidence that provides proof of computer voting equipment manipulation. With the increased use of DREs, there will be natural skepticism of the equipment since immediate paper trails associated with each independent vote are not apparent.

Most equipment manufacturers, in developing the current generation of paperless voting equipment, have designed and provided safeguards through audit logs and pre-election testing procedures that are equivalent to that of paper ballot handling equipment.

Copyright August, 2002

ATTACHMENT D

Central to the thrust of all current systems whether OMRs or DREs is the concept of ***"trust but verify"***. This means that a person who casts a vote receives instant verification that the vote cast is valid and that officials have the means to retrieve and examine such a vote at a later date if necessary.

In designing DRE equipment, manufacturers have followed the time-tested tenets of providing voter privacy and in ensuring that each individual voter's vote is counted in the form of "accuracy", "anonymity", "reliability" and "redundancy".

- Accuracy – That the votes are captured accurately and are verifiable at a later date. The system should also allow flexibility over time of changing ballot formats including write-in candidates, referendums and redistricting requirements, as well as "Challenge" or "Provisional" ballots. Modern DREs have eliminated the over-vote dilemma that was problematic during the 2000 elections.
- Anonymity – That each individual voter's privacy and anonymity rights are protected. This means that at the polls, no specific ballot is traceable to the individual voter who is qualified to cast a vote.
- Reliability – That voters are able to conveniently and efficiently cast votes with the confidence that the votes stored electronically can be replicated for tabulation without any votes being lost.
- Redundancy – In the event of systems failure that the data is backed up and can be reproduced and authenticated and that there are safeguards against unauthorized access.

Security Responsibilities

While there may be varying perception of possible tampering or wrong doing during the election planning, preparation and administration process, in reality election officials and election companies are committed to delivering secure and successful elections.

- Federal, State and Local Jurisdictions - With our nation's decentralized election system, elections are administered and conducted by local governments. Article I, Section 2 of the Constitution stipulates a limited role of federal power in this process. This sometimes inefficient election system is at times the best deterrence of any systematic effort to perpetrate large-scale fraud or voting equipment tampering.

  Given the fiduciary duty of election officials, most of whom are elected, to conduct credible and efficient elections, a system-wide breach of state or federal election would be extremely difficult at multiple sites, because different systems from multiple vendors would have to be compromised simultaneously.

Copyright August, 2002

- Voting Machine Manufacturers and Vendors - Operating in a full democracy's Free Market Economy, most election-related manufacturers, vendors and suppliers are incentivized by commerce and profit to develop and produce the most advanced, reliable election solutions in a competitive industry environment. Many manufacturers and vendors have longstanding, proven track records in the election business, which dictate their actions.

  Current federal funding legislation to overhaul the nation's election systems is pending. Manufacturers and vendors often benchmark each other and have a vested interest in delivering the most effective and efficient equipment employing quality assurance practices and thorough research and development methodologies.

  With public procurement procedures and certification requirements driving these competitive conditions, it is extremely difficult for any single manufacturer or vendor to manipulate or deviate from the voting equipment design requirements or functionalities.

Likewise, under these compelling circumstances, it would not be an overstatement to say that the election companies and elected officials have a "co-dependency" relationship. It is in the best interest of the equipment manufacturers to produce the most user-friendly products, to continually upgrade these voting systems, and for the jurisdictions to provide the requisite management control structures that ensure physical security and separation of duties.

While voters are not "direct influencers" of the election planning and administration processes, they should share the burden of being well informed about election security issues and procedures. This was evidenced by the voter outcry problems surrounding the 2000 elections. The availability of inaccurate information (sometimes misinformation) and increased Internet use further compounds this burden. Voter education and the understanding of equipment and methodology are imperative and paramount in providing transparency to the election security process.

Procurement Management

Experts have claimed that traditional public sector procurement models typically do not work well for information technology (IT) products. This is also true of computerized election system solutions and stems from the following reasons:

- There is usually a propensity to "under-purchase" on the part of jurisdictions. Costs of the new election systems do not always reflect

Copyright August, 2002

additional costs associated with integrating the system into existing IT structures and components. This creates a risk point for equipment rollout or implementation.

- Information technology system advancement often outpaces the procurement and implementation step, thus rendering the technology and equipment obsolete, or requiring continuous upgrades to meet current technology specifications.
- Large-scale information technology projects for elections are mass customization projects requiring the manufacturer or vendor to design very specific and unique solutions based on jurisdictional practices. This constraint is most reflective of the difficulty in consolidating national standards in voting systems solutions.

While the above does not pose as direct election security threats, most election companies work very closely with election officials based on the "co-dependency" model in bridging any information technology security risks.

This model requires both parties to be engaged early and often in the planning stages, to have IT decisions escalate to the highest-level decision makers who understand the process, and to have frequent progress evaluation and deliverables assessment milestones.

In addition, many jurisdictions have gone far down the road to building reliability and redundancy into their elections systems with the most appropriate IT equipment and operating systems with modularity, expandability, scalability and backup capabilities.

Finally, as complicated as information technology has become, election companies usually provide continuous training and skills development for the jurisdictions' IT personnel and equipment operators as part of the contract fulfillment and delivery process.

Voting Equipment and Software Safeguards

Prior to any official votes being cast, there are many safeguards and checks throughout the election preparation, tabulation and reporting cycle that election officials and the public can scrutinize regarding the accuracy and functionality of the voting equipment.

This process begins with certification of the election hardware, firmware and software, re-certification of any product upgrades, escrowing of the source code, public tests of the equipment prior to elections, and post Election Day testing.

Copyright August, 2002

ATTACHMENT D

Requirements of the Law

The Federal Election Commission (FEC) was formed in 1975 to administer and enforce the Federal Election Campaign Act (FECA) that governs the financing of federal elections. The FEC is an independent regulatory agency that has as its core function to conduct research activities. The FEC has recommendation authority to the Justice Department in the prosecution of FECA Finance Law violations.

The FEC sets guidelines for voting equipment certification through the Federal Voting Systems Standards (FVSS) and updates those standards to keep them dynamic to changes in technology and testing requirements. High level FEC guidelines related to the security of voting equipment derives from the following three sections:

- Section 3.2.2.1 (Administrative Database) states," The subsystem of any P&M or DRE system shall generate and maintain an administrative database containing the definitions and descriptions of political subdivisions and jurisdictions. The environment in which this database is operated shall include all necessary provisions for security and access control, and it shall ensure the security and access control of other databases in the system."

- Section 4.8.1 (Operational Requirements) states," Audit records shall be prepared for all phases of election operations. These records rely upon automated audit data acquisition and machine-generated reports, with manual input of some information. Primary emphasis is placed upon audit records of the ballot preparation and election definition phase, of system readiness tests, and of voting and ballot-counting operations. The software shall activate the logging and reporting of audit data as described in the following sections..."

- Section 5.3 (Access Control) states," All software (including firmware) for all voting systems shall incorporate measures to prevent access by unauthorized persons, and to prevent unauthorized operations by any person. Unauthorized operations include, but are not limited to: modification of compiled or interpreted code, run-time alteration of flow control logic or of data, and abstraction of raw or processed voting data in any form other than a standard output report by an authorized operator.

  Signatures on absentee ballots should be verified. Absentee ballots should be handled using the same security and tabulation procedures that apply to regular precinct ballots.

Copyright August, 2002

ATTACHMENT D

In addition to these design guidelines, the FEC also provides more specific physical security guidelines in Volume 1, Section 6 of its new Voting Systems Performance and Test Standards guidelines.

The FEC Equipment and Software Qualification Process

Certification is the process by which election equipment and software are measured against a set of documented specifications. Election equipment must be designed, coded and documented according to certification standards delineated in the FVSS. FVSS standards are voluntary, but often viewed as a minimum standard, as states can choose to enact stricter performance requirements for systems to be used in their jurisdictions.

There is both state and federal certification, with federal "qualification" preceding state certification. Most states follow FEC guidelines for state certification. For states that follow FEC guidelines, an election system must first meet FEC standards before it can be certified by the state.

To pass certification, a manufacturer assembles a Technical Data Package (TDP) that contains information on the products to be certified, including any change releases, manuals, technical specifications, software specifications and hardware/firmware specifications. The certification process from federal qualification to state certification is as follows:

- The FEC coordinates with the National Association of State Election Directors (NASED) to select and approve an Independent Testing Authority (ITA) to conduct review and testing of the voting equipment and software seeking certification.

  NASED is an organization of state election administrators. The organization does not have authority over the FVSS or individual components of the standards but does administer the FEC guidelines and select and qualify the ITAs. ITAs are independent testing laboratories that perform thorough mechanical, functional and source code testing measuring the FVSS against the voting system's own specifications.

- The ITA tests include an in-depth examination of the software, an inspection and evaluation of system documentation; tests of hardware under conditions simulating the intended storage, operation, transportation, and maintenance environments; and operational tests verifying system performance and function under normal and abnormal conditions. Once the equipment or software is completely through the testing process, it receives a NASED Qualified Identification Number.

Copyright August, 2002

Once qualified, the manufacturers or vendors can apply to individual states for certification. The tests involved in state certification differ from those required for FEC qualification. The FEC qualification tests the functionality of the equipment. The state tests are used to make sure that election equipment complies with specific election laws and practices established by the state where the system is to be sold.

All vendors must meet the same tests for qualification. Each required test is performed identically by the ITAs for manufacturer so that no vendor holds an advantage over others in the type of testing performed. Manufacturer and vendors are not qualified; instead specific systems are qualified.

In order to maintain its status as a NASED qualified system, the hardware, firmware and software cannot deviate from the original version of what was tested by the ITAs, or risk being in noncompliance with the state's certification process.

State Level Testing and Certification

Most states have substantial election fraud enforcement authority, usually through the State Attorney General's offices. Several states have extremely strong anti-fraud statues with large agencies and staffs, such as New York. However, these resources do not necessarily devote attention to the technical functions of voting equipment and software. That function is delegated to the technical administrators of the state's division of elections.

At the state level, for both hardware and software products, when a manufacturer or vendor decides to upgrade versions or sell a new product in particular states, they need to apply or reapply to the state's division of elections for approval through a new TDP for each certification. Additionally, some states require process flow diagrams and written documentation of this process.

After the TDP is reviewed and determined complete, a date is scheduled for testing. In the interim, the manufacturer or vendor works out detailed requirements for the specific certification with the state. Machine coding, ballot layout and hardware are prepared and internal testing conducted.

State certification testing is stringent. Most election systems are required to be re-certified whenever code changes are made to software or firmware. During the test period, machines and software are held to rigid performance standards as stated in the TDP, and the examination observed at all times by technical and non-technical representatives from the state. Certification is not automatic and often requires additional improvements and retests using the same rigid standards. Some products never achieve certification.

Copyright August, 2002

ATTACHMENT D

Software Source Code and Security

Contrary to the public's common misconceptions pertaining to proprietary computer programs, manufacturers and vendors that develop and provide election-related software are often required to escrow these software source code with a third party depository. The claim of protection of proprietary intellectual property rights is not valid in this case as data redundancy, accessibility and the public trust is involved.

Election-related software includes vote tabulation software and election management software. NASED defines software as "software... that are not in a permanent machine resident status, such as on a Read Only Memory chip. This includes software that is resident on a computer hard drive or any software that is external to the voting system".

The obligation and benefits of depositing specific election source code with software escrow companies are twofold:

1. In the event of cataclysmic events to the software provider, the original source code in the form of magnetic tape, disk, or other tangible media are available for replacement because these programs are stored elsewhere in secure, environmentally-safe, locked facilities with authorized access.
2. As part of the escrow process, jurisdictions that use the particular escrowed software do have access to the source code to inspect, validate or conduct random review of this source code in conjunction with the vendors. If any questions arise after an election, the escrowed source codes can be compared against the election software to detect security breaches or inconsistencies.

While there remain doubters of the software security process, it is important to understand that election software development, testing and approval often are team efforts with proper handoffs and crosschecks. Doubters cite potential problems of tampering with the compiler's source code or implantation of "bugs" by individual programmers. In reality, during the election company's development and testing process, the software undergoes numerous regression, beta, integration and systems tests before it goes to FEC qualification. During qualification, the ITAs take possession of the source code to independently verify, [illegible] software and these are the actual software [illegible] eliminate the [illegible]

[illegible] the purpose and intent of crosschecks [illegible] the certification process, the requirement for source code escrows and the access available to the [illegible] would be difficult for any [illegible]

Copyright August 2002

ATTACHMENT D

programs once they have been presented or certified by the state testing authorities.

Jurisdictional Testing Requirements

Aside from certification to assure that security measures are in place prior to any election, there is no substitute for testing and dry runs. Testing and re-testing flushes out any physical interference or procedural breaches and can ensure the accuracy of election results as well as test for data transmission connectivity and security. These tests are conducted and observed by jurisdictional officials and election boards to determine if any discrepancy exists between hardware, software and the ballots voted.

At minimum, most jurisdictions require a combination of the following:

- Audit Data Trail – The "Audit Log Report" or "Audit Log", is an internal report that tracks all OMR or DRE software actions from the moment a voting system is started to the time it is turned off, regardless of multiplicity. The "Audit Log" is generated in real time and cannot be altered or reproduced. This test tracks and records every single action on the equipment.

- Public Count – This an ongoing, incremental record of the total number of voters who have voted on an OMR ballot or DRE terminal from the time the terminal was opened on Election Day or during testing. Set to zero before each election or test, the public count is incremented and displayed on each machine throughout Election Day or during a test.

  A "zero tape" produced by the machine prior to the opening of polls or test verifies that the public count of each terminal was set at zero and at the close of polls or test. For DREs, the same machine is required to provide a printed report of all votes that were cast on individual DRE terminals and for all terminals employed in an Election Day precinct. In an actual election the public count can be used throughout the day for crosschecking with the number of voters recorded in the Poll Book.

- Logic & Accuracy Tests – Conducted much like an actual election, or a "Mock Election", this test runs all of the available Ballot Styles (the specific precinct/district/jurisdiction of the ballot) voted and compares these results against the actual marked ballots or votes used to test equipment accuracy. The testing is conducted to confirm that the Election Definition (the set of contest and candidate variables defined by each election) programmed into the voting equipment accurately performs for the specific election. This test is a quality assurance procedure as well as a security assurance one.

Copyright August, 2002

In conjunction with the above tests, some jurisdictions also conduct simultaneous "stress tests" by subjecting the voting equipment to many types of potential disruptions during the vote tabulation and report generation phase, including power supply disruptions, abnormal humidity and temperature conditions, etc.

Given the jurisdictional requirements set for acceptance of ballot and programming quality and delivery, and the scrutiny and supervision of tests, it would be difficult for any manufacturer or vendor to tamper with the accuracy of the voting equipment or software.

Ballot Security and Accountability

For OMR voting systems, ballot security and accountability assures the integrity of the election process. The responsibility and control of the ballots during the pre-election preparation phase falls back to the "codependency model" between the jurisdictions and election companies. This shared responsibility for the ballots' physical security often is in the form of sign off documentation throughout the code stock printing, ballot layout, production, transfer, and storage procedures.

There are two tiers of ballot security and accountability requirements in the form of State laws and State rules or regulations. Because ballots can be handled much like security papers, there are currently no major issues related to the physical accounting of ballots.

On Election Day and beyond, the responsibility for ballot security and accountability reverts back to the jurisdiction for proper transfer and handling of ballots to and from the polling places, collection and control of voted and unused ballots, and procedures related to final ballot tabulation. This includes the increased usage of non Election Day ballots in the form of Postal Early Voting, Challenge and Provisional ballots. Oregon, for example, currently holds all-mail ballot elections.

In OMR operations, the ballots are scanned through the OMR machines. Most machines use preprogrammed memory devices, such as Erasable Programmable Read Only Memory (EPROM) chips or zip disks as interfaces for the voted marks to be detected. These memory devices are programmed by authorized personnel prior to an election and are also guarded much like secured ballots.

With the increased adoption of DRE equipment by many jurisdictions, some have predicted the eventual obfuscation of paper ballots, which will alleviate the security burdens and costs associated with paper ballots. This may or may not be the case as indicated earlier with the increases in Postal Early Voting.

Copyright August, 2002

Tamper Prevention at the Polling Place

Much like the secure or locked ballot box on Election Day, equipment manufacturers have adopted state-of-the-art technology to include safety features that prevent equipment tampering at the polling places where there is direct public access to the voting devices.

At the jurisdictional level, physical security prior to Election Day include well maintained warehouses and secure equipment loading and staging areas, sealed and locked voting equipment, devices and voting booths and limited access to computer rooms and central tabulation facilities by non election related personnel.

Most election officials take the additional precaution of safeguarding data lines and file transfers during the election preparation process with secure firewalls, data encryption and protocols. The most astute jurisdiction also ensures that no one individual controls all election procedures, by assigning the duties to many individuals for different phases of the process. Others further restrict access to the dissemination of election results until they are verified.

On Election Day, for a ballot to be cast properly, the voting devices need to be activated for individual voters either by precinct officials or by the voters independently. Precinct based paper voting usually allows the voter to interact directly with the machine, while electronic voting can be either poll worker activated or voter activated depending on jurisdictional law. In both ballot loading systems, activating more than one ballot for any given voter is not possible.

- For OMR ballots, some manufacturers have built-in features within the optical scanners that detect the sheet thickness of the ballots. This feature identifies and stops the machines whenever a non-standard ballot or the presence of more than one ballot is detected and informs the voter or poll official that there are wrong ballots or multiple ballots in the counter. Ballot style codes printed on the ballots and programmed in the machines prevent the acceptance of erroneous ballots and damaged ballots that are not designated to the specific polling places.

- For electronic voting, the DRE machines use non-standard election specific operating systems in combination with proprietary software to interface the activation of the machines with Personal Computer Memory Card International Association (PCMCIA) cards, Infrared Ballot Activator cartridges or Smart Cards. These activator devices are not common to the PC environment and require the authentication by the machine's software and firmware for them to function. Without pre-qualified activator devices the machines will not operate. Any attempts at tampering with these devices will also render the machines inoperative. These activator devices, because of

Copyright August, 2002

their value in activating the machines are in the custody of appropriate election officials once they are programmed.

To prevent the unauthorized opening or closing of polls outside of the official poll hours, DRE machines are also equipped with sequential passwords to fend off any such action. The machines' audit logs, naturally will record any such attempts.

Zero Vote Reports

Prior to Election Day, once Election Definitions and ballots formats are loaded into the voting equipment and machine accuracy is verified through public tests, a final zero vote report tied to the specific equipment is usually produced to validate that the machine was set at zero. This test is conducted prior to polls opening. To minimize the opportunity for tampering, good management controls utilize separation of duties or crosschecks.

Post election, many jurisdictions use electronic data transmissions to transfer results directly from their precincts. To prevent file corruption during electronic transmission of results to election central, log in and password codes are required to prevent any tampering of files during transit. In the transmission of results using proprietary protocols, if any file corruption is detected, that file transmission will be interrupted and rejected.

Post Election Day Testing

Post Election Day, recounts and canvassing requirements serve as additional validation mechanism for the security of voting equipment.

Currently, 17 states have mandatory recounts rules and 30 others allow for recounts under varying situations. Connecticut, Delaware and New York are the only three states that prohibit recounts.

Canvassing involves a group of jurisdictional officials who are responsible for verifying that the number of ballots cast on Election Day is equal to those counted on election night.

In this sense, vote "accuracy", "anonymity", "reliability" and "redundancy" constitute the final test for any computerized voting equipment.

For OMR equipment, electronic re-tabulation of the ballots can be conducted by rescanning the same ballots using the same equipment or a compatible model. The results are then compared on a precinct-by-precinct basis with the original

Copyright August, 2002

ATTACHMENT D

tally. Alternatively, a manual recount can be conducted by hand counting all ballots, and then comparing the results on a precinct-by-precinct basis.

For DRE equipment the process is actually quite similar as individual ballot images can be generated and printed if necessary to recover the ballots for a hand recount. Typically, ballot images are stored on different chips within the machine and intermittently crosschecked for completeness against each other for accuracy.

These ballot images, coupled with the chronological report supplied by the audit log of machine functionalities, provide a complete and accurate picture of every event that occurred on the machines.

Conclusion

Despite any public perception to the contrary, the checks and balances for election equipment tamper detection and prevention process are in place.

Through FEC guidelines and certification requirements, manufacturers and vendors are continually pushed to develop and produce the most effective equipment to safeguard the public's vote and are conscientious about doing so. Additional safeguard mechanisms in the form of re-certification, public tests and post Election Day testing to verify the functionalities of the equipment are the norm in the industry

Election security does require the public to "trust but verify", with vigilant, informed voters and responsible election administrators. Any voting system is only as secure and dependable as the people who administer and operate the equipment.

References

Carter, Jimmy, et al (2002). "To Assure Pride and Confidence in the Electoral Process/Report of the National Commission on Federal Election Reform". Brookings Institution: Washington D.C.

Cornish, Jay (2000). "Improving the Procurement Process: National Computerized Election Systems". *2000 IFES Buyer's Guide to Election Suppliers.* International Foundation for Election Systems (IFES): Washington, D.C.

Copyright August, 2002

ATTACHMENT D

Donsanto, Craig and Stewart, Nancy; Ingersoll, Nancy, Editor. (1995). "Federal Prosecution of Election Offenses". United States Department of Justice. Public Integrity Section: Washington D.C.

Dudley, Robert and Gitelson, Alan (2002). "American Elections: The Rules Matter". Longman Publishers: New York.

Duncan, Guy (2002). "Benefits and Limitations of Online Voting". *Internet Voting White Paper.* Election System and Software: Omaha, NE.

Gerber, Marie; Kimberling, William, Editor (1995). "Ballot Security and Accountability". National Clearinghouse on Election Administration, Federal Election Commission: Washington D. C.

Gerck, Ed. Editor (2001). "Voting System Requirements". *The Bell: Privacy, Security and Technology in Internet Voting.* Februaury 2001, Vol.2 No. 2

Kamarck, Elaine and Nye, Joseph, Editors (2002). "Governance.com: Democracy in the Information Age; Visions of Governance in the Information Age". Brookings Institutions Press: Washington D. C.

Keikkila, Ralph; Kimberling, William, Editor (1995). "The Electronic Transmission of Election Materials". National Clearinghouse on Election Administration, Federal Election Commission: Washington D. C.

National Association of State Election Directors. "General Overview for Getting a Voting System Qualified". http://www.nased.org/ITA_process.htm

Saltman, Roy (1988). "Accuracy, Integrity, and Security in Computerized Vote-Tallying". United States Department of Commerce. National Bureau of Standards: Gaithersburg, MD

Thompson, Ken (1990) "Reflections on Trusting Trust". *Computers Under Attack: Intruders, Worm, and Viruses.* Copyright ACM Press.

FLORIDA DEPARTMENT OF STATE
Glenda E. Hood
Secretary of State

December 15, 2003

The Honorable Bob Graham
United States Senate
524 Hart Senate Office Building
Washington, DC 20510

Dear Senator Graham:

As Florida's chief elections officer, I share your commitment to a smooth election process and protecting every citizens' right to vote. That is why I was disappointed to learn the details of Senate Bill 1980 that you filed, requiring paper documentation of every vote cast across the country by the November 2004 election.

Although well intentioned, if passed your legislation would present significant obstacles in the upcoming 2004 election cycle.

Before I share my concerns about this bill, let me assure you that Florida has implemented election reform that is second to none. Since the 2000 election, the Florida Legislature has passed, and our 67 Supervisors of Elections have implemented, efforts that have made us a leader in this regard. Our touch screen voting equipment has passed the certification standards of the United States Government and the Florida Department of State Division of Elections office, which has one of the highest certification standards in the nation. The machines we have certified are secure against tampering and fraudulent manipulation. It is these very machines that were used successfully in Florida's 2002 primary and general elections. We are confident they will also be used successfully in the 2004 primary and general elections.

As it relates to Senate Bill 1980, I trust you are aware that only one vendor in the entire country offers a paper audit trail system. This vendor has not applied for certification in our state. Additionally, the paper audit system – unlike the optical scan and touch screen voting machines – is untried in any official election. The 2004 general election would not be the appropriate testing ground for these devises.

Equally troubling is the logistical snafu your legislation would present. Today we are only eleven months from the 2004 general election. Should SB 1980 pass, the country's one vendor would need first to apply for and be certified by federal and state governments, and second would have to manufacture and distribute their machines throughout the country. Florida alone has 6,700 precincts, to say nothing of the nation as a whole. Additionally, local counties would need to approve the increased costs of these systems as well as provide additional training for their poll workers.

R. A. Gray Building • 500 S. Bronough • Tallahassee, Florida 32399-0250 • (850) 245-6500
http://www.dos.state.fl.us

Senator Graham, I urge you not to rush forward with legislation whose consequences are unknown. A better course would be to allow the National Institute for Standards and Technology, which is charged with developing election system criteria, to complete its work. At this moment, the Institute is working with voting and election stakeholders to evaluate and develop new standards based on the latest technological developments. Make no mistake about it, these are uncharted waters. Until standards and technology are developed, tested and approved, it is irresponsible to place an unrealistic timeline on our country, our state and our 67 Supervisors of Elections. Also damaging is the adverse impact this legislation would have in the confidence Florida voters have in the current system.

In a 2002 Election Night Statewide Survey poll commissioned by The Collins Center for Public Policy and the James Madison Institute, when voters were asked if they were confident their vote counted in the 2002 election, an overwhelming 95.2 percent responded favorably. Of those who responded, 52.4% used touch screen machines, 18% used optical scan machines, with 25.7% voting by absentee.

Let us not take a step backward by instilling fear and doubt in a system that has been successful for our state's 9.3 million registered voters.

Sincerely,

Glenda E. Hood

Glenda E. Hood

The Capitol • Tallahassee, Florida 32399-0250 • (850) 245-6500
http://www.dos.state.fl.us

Analysis of an Electronic Voting System

Tadayoshi Kohno
Information Security Institute
Johns Hopkins University
yoshi@cs.jhu.edu

Adam Stubblefield
Information Security Institute
Johns Hopkins University
astubble@cs.jhu.edu

Aviel D. Rubin
Information Security Institute
Johns Hopkins University
rubin@cs.jhu.edu

Dan S. Wallach
Department of Computer Science
Rice University
dwallach@cs.rice.edu

July 23, 2003

Abstract

Recent election problems have sparked great interest in managing the election process through the use of electronic voting systems. While computer scientists, for the most part, have been warning of the perils of such action, vendors have forged ahead with their products, claiming increased security and reliability. Many municipalities have adopted electronic systems, and the number of deployed systems is rising. For these new computerized voting systems, neither source code nor the results of any third-party certification analyses have been available for the general population to study, because vendors claim that secrecy is a necessary requirement to keep their systems secure. Recently, however, the source code purporting to be the software for a voting system from a major manufacturer appeared on the Internet. This manufacturer's systems were used in Georgia's state-wide elections in 2002, and the company just announced that the state of Maryland awarded them an order valued at up to $55.6 million to deliver touch screen voting systems.[1]

This unique opportunity for independent scientific analysis of voting system source code demonstrates the fallacy of the closed-source argument for such a critical system. Our analysis shows that this voting system is far below even the most minimal security standards applicable in other contexts. We highlight several issues including unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, and poor software development processes. For example, common voters, without any insider privileges, can cast unlimited votes without being detected by any mechanisms within the voting terminal. Furthermore, we show that even the most serious of our outsider attacks could have been discovered without the source code. In the face of such attacks, the usual worries about insider threats are not the only concerns; outsiders can do the damage. That said, we demonstrate that the insider threat is also quite considerable. We conclude that, as a society, we must carefully consider the risks inherent in electronic voting, as it places our very democracy at risk.

[1] http://www.corporate-ir.net/ireye/ir_site.zhtml?ticker=DBD&script=410&layout=-6&item_id=433030

1 Introduction

The essence of democracy is that everyone accepts the results of elections, even when they lose them. Elections allow the populace to choose their representatives and express their preferences for how they will be governed. Naturally, the integrity of the election process is fundamental to the integrity of democracy itself. And, unsurprisingly, history is littered with examples of elections being manipulated in order to influence their outcome.

The design of a "good" voting system, whether electronic or using traditional paper ballots or mechanical devices, must be robust against a wide variety of potentially fraudulent behavior. The *anonymity* of a voter's ballot must be preserved, both to guarantee the voter's safety when voting against a malevolent candidate, and to guarantee that voters have no evidence that proves which candidates received their votes. The existence of such evidence would allow votes to be purchased by a candidate. The voting system must also be *tamper-resistant* to thwart a wide range of attacks, including ballot stuffing by voters and incorrect tallying by insiders. Another important consideration, as shown by the so-called "butterfly ballots" in the Florida 2000 presidential election, is the importance of *human factors*. A voting system must be comprehensible to and usable by the *entire* voting population, regardless of age, infirmity, or disability. Providing accessibility to such a diverse population is an important engineering problem and one where, if other security is done well, electronic voting could be a great improvement over current paper systems. Flaws in any of these aspects of a voting system, however, can lead to indecisive or incorrect election results.

1.1 Electronic voting systems

There have been several studies on using computer technologies to improve elections [Cal01, Cal00, Mer00, Nat01, Rub02]. These studies caution about the risks of moving too quickly to adopt electronic voting machines because of the software engineering challenges, insider threats, network vulnerabilities, and the challenges of auditing.

As a result of the Florida 2000 presidential election, the inadequacies of widely-used punch card voting systems have become well understood by the general population. This has led to increasingly widespread adoption of "direct recording electronic" (DRE) voting systems. DRE systems, generally speaking, completely eliminate paper ballots from the voting process. As with traditional elections, voters go to their home precinct and prove that they are allowed to vote there, perhaps by presenting an ID card, although some states allow voters to cast votes without any identification at all. After this, the voter is typically given a PIN or a smartcard or some other token that allows them to approach a voting terminal, enter the PIN or smartcard, and then vote for their candidates of choice. When the voter's selection is complete, DRE systems will typically present a summary of the voter's selections, giving them a final chance to make changes. Subsequent to this, the ballot is "cast" and the voter is free to leave.

The most fundamental problem with such a voting system is that the entire election hinges on the correctness, robustness, and security of the software within the voting terminal. Should that code have security-relevant flaws, they might be exploitable either by unscrupulous voters or by malevolent insiders. Such insiders include election officials, the developers of the voting system, and the developers of the embedded operating system on which the voting system runs. If any party introduces flaws into the voting system software or takes advantage of pre-existing flaws, then the results of the election cannot be assured to accurately reflect the votes legally cast by the voters.

The only known solution to this problem is to introduce a "voter-verifiable audit trail." [DMNW03]. Most commonly, this is achieved by adding a printer to the voting terminal. When the voter finishes selecting candidates, a ballot is printed on paper and presented to the voter. If the printed ballot reflects the voter's intent, the ballot is saved for future reference. If not, the ballot is mechanically destroyed. Using this "Mercuri method," [Mer00] the tally of the paper ballots takes precedence over any electronic tallies. As

a result, the correctness of the voting terminal software no longer matters; either a voting terminal prints correct ballots or it is taken out of service.

1.2 "Certified" DRE systems

Many government entities have adopted paperless DRE systems without appearing to have critically questioned the security claims made by the systems' vendors. Until recently, such systems have been dubiously "certified" for use without any public release of the analyses behind these certifications, much less any release of the source code that might allow independent third parties to perform their own analyses. Some vendors have claimed "security through obscurity" as a defense, despite the security community's universally held belief in the inadequacy of obscurity to provide meaningful protection.

"Security through obscurity" is a long-rejected theory that systems can be made more secure by simply hiding the security mechanisms from public view. While this theory has some validity in situations where the need for security is not great — hiding a spare key to a liquor cabinet just out of sight of small children — the theory has been soundly rejected as a means of serious security [Ker83]. This is because it has the twin faults of not providing serious security from real attackers, who can easily overcome minimal security measures, and of limiting public and general security oversight of the system, which has proven to be the best method for creating and maintaining a truly secure system [Sch00].

Indeed, source code that appears to correspond to a version of Diebold's voting system appeared recently on the Internet. This appearance, announced by Bev Harris and discussed in her book, *Black Box Voting* [Har03], gives us a unique opportunity to analyze a widely used, paperless DRE system and evaluate the manufacturer's security claims.

To the best of our knowledge, the code (hereafter referred to as the "Diebold code") was discovered by others on a publicly available Diebold ftp site in January, 2003. It has since been copied to other sites around the world and its release has been the subject of numerous press reports. To the authors' knowledge, Diebold has raised no objection to the broad publication and republication of the code to date. Jones discusses the origins of this code in extensive detail [Jon03].

The security of Diebold's voting system is of growing concern as on July 21, 2003, the company finalized an agreement for up to $55.6 million to deliver touch-screen voting technology to the state of Maryland. The contract includes about 11,000 Diebold touch-screen voting systems. Diebold voting systems were also used in state-wide elections in Georgia in 2002.

1.3 Summary of results

We only inspected unencrypted source code that we believe was used in Diebold's AccuVote-TS voting terminal [Die03] (the "AVTSCE" tree in the CVS archive). We have not independently verified the current or past use of the code by Diebold or that the code we analyzed is actually Diebold code, although as explained further in Section 6.1, the copyright notices and code legacy information in the code itself are consistent with publicly available systems offered by Diebold and a company it acquired in 2001, Global Election Systems. Also, the code itself built and worked as an election system consistent with Diebold's public descriptions of its system. We concluded that even if it turned out that the code was not part of a current or past Diebold voting system, analysis of it would be useful to the broader public debate around electronic voting systems security and assist election officials and members of the public in their consideration of not only Diebold systems, but other electronic voting systems currently being marketed nationwide and around the world. We did not have source code to Diebold's GEMS back-end election management system.

Furthermore, we only analyzed source code that could be directly observed and copied from the CVS software archive without further effort. A large amount of the other data made publicly available was protected by very weak compression/encryption software known as PKZip, which requires a password for

access to the underlying work. PKZip passwords are relatively easy to avoid, and programs for locating passwords for PKZip files are readily available online. Moreover, passwords that others have located for these files have been freely available online for some time. Nonetheless, we decided to limit our research to only the files that were publicly available without any further effort, in part due to concerns about possible liability under the anti-circumvention provisions of the Digital Millennium Copyright Act.

Even with this restricted view of the source code, we discovered significant and wide-reaching security vulnerabilities in the AccuVote-TS voting terminal. Most notably, voters can easily program their own smartcards to simulate the behavior of valid smartcards used in the election. With such homebrew cards, a voter can cast multiple ballots without leaving any trace. A voter can also perform actions that normally require administrative privileges, including viewing partial results and terminating the election early. Similar undesirable modifications could be made by malevolent poll workers (or even maintenance staff) with access to the voting terminals before the start of an election. Furthermore, the protocols used when the voting terminals communicate with their home base, both to fetch election configuration information and to report final election results, do not use cryptographic techniques to authenticate the remote end of the connection nor do they check the integrity of the data in transit. Given that these voting terminals could communicate over insecure phone lines or even wireless Internet connections, even unsophisticated attackers can perform untraceable "man-in-the-middle" attacks.

As part of our analysis, we considered both the specific ways that the code uses cryptographic techniques and the general software engineering quality of its construction. Neither provides us with any confidence of the system's correctness. Cryptography, when used at all, is used incorrectly. In many places where cryptography would seem obvious and necessary, none is used. More generally, we see no evidence of rigorous software engineering discipline. Comments in the code and the revision change logs indicate the engineers were aware of areas in the system that needed improvement, though these comments only address specific problems with the code and not with the design itself. We also saw no evidence of any change-control process that might restrict a developer's ability to insert arbitrary patches to the code. Absent such processes, a malevolent developer could easily make changes to the code that would create vulnerabilities to be later exploited on Election Day. We also note that the software is written entirely in C++. When programming in an unsafe language like C++, programmers must exercise tight discipline to prevent their programs from being vulnerable to buffer overflow attacks and other weaknesses. Indeed, buffer overflows caused real problems for AccuVote-TS systems in real elections.[2]

2 System overview

Although the Diebold code is designed to run on a DRE device (an example of which is shown in Figure 1), one can run it on a regular Microsoft Windows computer (during our experiments we compiled and ran the code on a Windows 2000 PC).

In the following we describe the process for setting up and running an election using the Diebold system. Although we know exactly how the code works from our analysis, we must still make some assumptions about the external processes at election sites. In all such cases, our assumptions are based on the way the Diebold code works, and we believe that our assumptions are reasonable. There may, however, be additional administrative procedures in place that are not indicated by the source code. We first describe the architecture at a very high level, and then, in Section 2.1 we present an overview of the code. Since the Diebold code can be run both on DRE devices and PCs, we shall refer to a device running the vote collection software as a *voting terminal*.

SETTING UP. Before an election takes place, one of the first things the election officials must do is specify the

[2] `http://www.sccgov.org/scc/assets/docs/209815KeyboardAttachment-200440211.pdf` (page 48)

ATTACHMENT F

	Voter (with forged smartcard)	Poll Worker (with access to storage media)	Poll Worker (with access to network traffic)	Internet Provider (with access to to network traffic)	OS Developer	Voting Device Developer	Section
Vote multiple times using forged smartcard	•	•	•				3.1.1
Access administrative functions or close polling station	•	•			•	•	3.1.2
Modify system configuration		•			•	•	4.2
Impersonate legitimate voting machine to tallying authority		•	•	•	•	•	4.3
Modify ballot definition (e.g., party affiliation)		•	•	•	•	•	4.3 and 5.1
Cause votes to be miscounted by tampering with configuration		•	•	•	•	•	4.3 and 5.1
Tamper with audit logs		•			•	•	4.4
Create, delete, and modify votes on device		•			•	•	4.4
Link votes to voters		•			•	•	4.4
Delay the start of an election		•	•	•	•	•	5.2
Tamper with election results		•	•	•	•	•	5.2
Insert backdoors into code					•	•	6.3

Table 1: This table summarizes some of the more important attacks on the system.

58

Figure 1: A Diebold DRE Voting Machine (photo from `http://www.sos.state.ga.us/`). Note the smartcard reader in the lower-right hand corner.

political offices and issues to be decided by the voters along with the candidates and their party affiliations. Variations on the ballot can be presented to voters based on their party affiliations. We call this data a *ballot definition*. In the Diebold system, a ballot definition is encoded as the file `election.edb` and stored on a back-end server.

Shortly prior to the election, the voting terminals must be installed at each voting location. In common usage, we believe the voting terminals will be distributed without a ballot definition pre-installed. Instead, a governmental entity using Diebold voting terminals has a variety of choices in how to distribute the ballot definitions. They may be distributed using removable media, such as floppy disks or storage cards. They may also be transmitted over the Internet or a dial-up connection. This provides additional flexibility to the election administrator in the event of last-minute changes to the ballot.

THE ELECTION. Once the voting terminal is initialized with the ballot definitions, and the election begins, voters are allowed to cast their votes. To get started, however, the voter must have a *voter card*. The voter card is a memory card or smartcard; i.e., it is a credit-card sized plastic card with a computer chip on it that can store data and, in the case of the smartcard, perform computation. We do not know exactly how the voter gets his voter card. It could be sent in the mail with information about where to vote, or it could be given out at the voting site on the day of the election. To understand the voting software itself, however, we do not need to know what process is used to distribute the cards to voters.

The voter takes the voter card and inserts it into a smartcard reader attached to the voting terminal. The terminal checks that the smartcard in its reader is a voter card and, if it is, presents a ballot to the voter on the terminal screen. The actual ballot the voter sees may depend on the voter's political party, which is encoded on the voter card. If a ballot cannot be found for the voter's party, the voter is given a nonpartisan ballot.

At this point, the voter interacts with the voting terminal, touching the appropriate boxes on the screen for his or her desired candidates. Headphones are available for visually-impaired voters to privately interact with the terminal. Before the ballots are committed to storage in the terminal, the voter is given a final chance to review his or her selections. If the voter confirms this, the vote is recorded on the voting terminal and the voter card is "canceled." This latter step is intended to prevent the voter from voting again with the same card. After the voter finishes voting, the terminal is ready for another voter to use.

REPORTING THE RESULTS. A poll worker ends the election process by inserting an *administrator card* or an *ender card* (a special card that can only be used to end the election) into the voting terminal. Upon detecting the presence of such a card (and, in the case of the administrator card, checking a PIN entered by the card user), the poll worker is asked to confirm that the election is finished. If the poll worker agrees, then the voting terminal enters the post-election stage and can transmit its results to the back-end server.

As we have only analyzed the code for the Diebold voting terminal, we do not know exactly how the back-end server tabulates the final results it gathers from the individual terminals. Obviously, it collects all the votes from the various voting terminals. We are unable to verify that there are checks to ensure, for example, that there are no more votes collected than people who are registered at or have entered any given polling location.

2.1 Details

We now describe the Diebold system in more detail, making explicit references to the relevant portions of the code. The voting terminal is implemented in the directory `BallotStation/`, but uses libraries in the supporting directories `Ballot/`, `DES/`, `DiagMode/`, `Shared/`, `TSElection/`, `Utilities/`, and `VoterCard/`.

The method `CBallotStationApp::DoRun()` is the main loop for the voting terminal software. The `DoRun()` method begins by invoking `CBallotStationApp::LoadRegistry()`, which loads information about the voting terminal from the registry (the registry keys are stored under `HKEY_LOCAL_`

MACHINE\Software\GlobalElectionSystems\AccuVote-TS4). If the program fails to load the registry information, it believes that it is uninitialized and therefore creates a new instance of the CTSRegistryDlg class that asks the administrator to set up the machine for the first time. The administrator chooses, among other things, the COM port to use with the smartcard reader, the directory locations to store files, and the polling location identifier. The CBallotStationApp::DoRun() method then checks for the presence of a smartcard reader and, if none found, gives the administrator the option to interact with the CTSRegistryDlg again.

The DoRun() method then enters a while loop that iterates until the software is shut down. The first thing DoRun() does in this loop is check for the presence of some removable media on which to store election results and ballot configurations (a floppy under Windows or a removable storage card on a Windows CE device). It then tries to open the election configuration file election.edb. If it fails to open the configuration file, the program enters the CTSElectionDoc::ES_NOELECTION state and invokes CBallotStationApp::Download(), which creates an instance of CTransferElecDlg to download the configuration file. To do the download, the terminal connects to a back-end server using either the Internet or a dial-up connection. The program then enters the CTSElectionDoc::ES_PREELECT state, invokes the CBallotStationApp::PreElect() method, which in turn creates an instance of CPreElectDlg. The administrator can then decide to start the election, in which case the method CPreElectDlg::OnSetForElection() sets the state of the terminal to CTSElectionDoc::ES_ELECTION.

Returning to the while loop in CBallotStationApp::DoRun(), now that the machine is in the state CTSElectionDoc::ES_ELECTION, the DoRun() method invokes CBallotStationApp::Election(), which creates an instance of CVoteDlg. When a card in inserted into the reader, the reader checks to see if the card is a voter card, administrator card, or ender card. If it is an ender card, or if it is an administrator card and if the user enters the correct PIN, the CVoteDlg ends and the user is asked whether he wishes to terminate the election and, if so, the state of the terminal is set to CTSElectionDoc::ES_POSTELECT. If the user entered a voter card, then DoVote() is invoked (here DoVote() is an actual function; it does not belong to any class). The DoVote() function finds the appropriate ballot for the user's voter group or, if none exists, opens the nonpartisan ballot (recall that the system is designed to allow voters to vote by group or party). It then creates an instance of CBallotDlg to display the ballot and collect the votes.

We recall that if, during the election process, someone inserted an administrator or ender card into the terminal and choses to end the election, the system would enter the CTSElectionDoc::ES_POSTELECT state. At this point the voting terminal would offer the ability to upload the election results to some back-end server for final tabulation. The actual transfer of results is handled by the CTransferResultsDlg::OnTransfer() method.

We will present more details about the Diebold system in the following sections.

3 Smartcards

While it is true that one can design secure systems around the use of smartcards, simply the use of smartcards in a system does *not* imply that the system is secure. The system must use the smartcards in an intelligent and security-conscious way. Unfortunately, the Diebold system's use of smartcards provides very little (if any) additional security and, in fact, opens the system to several attacks.

3.1 Homebrew smartcards

Upon reviewing the Diebold code, we observed that the smartcards do not perform any cryptographic operations.[3] For example, authentication of the terminal to the smartcard is done "the old-fashioned way:" the terminal sends a cleartext (i.e., unencrypted) 8-byte password to the card and, if the password is correct, the card believes that it is talking to a legitimate voting terminal. Unfortunately, this method of authentication is insecure: an attacker can easily learn the 8-byte password used to authenticate the terminal to the card (see Section 3.3), and thereby communicate with a legitimate smartcard using his own smartcard reader.

Furthermore, there is no authentication of the smartcard to the device. This means that nothing prevents an attacker from using his own homebrew smartcard in a voting terminal. One might naturally wonder how easy it would be for an attacker to make such a homebrew smartcard. First, we note that many smartcard vendors sell cards that can be programmed by the user. An attacker who knows the protocol spoken by the voting terminal to the legitimate smartcard could easily implement a homebrew card that speaks the same protocol. Even if the attacker does not *a priori* know the protocol, an attacker could easily learn enough about the protocol to create new voter cards by attaching a "wiretap" device between the voting terminal and a legitimate smartcard and observing the communicated messages. The parts for building such a device are readily available and, given the privacy of voting booths, might be unlikely to be noticed by poll workers. An attacker might not even need to use a wiretap to see the protocol in use. Smartcards generally use the ISO 7816 standard smartcard message formats. Likewise, the important data on the legitimate voting card is stored as a file (named `0x3D40` — smartcard files have numbers instead of textual file name) that can be easily read by a portable smartcard reader. Again, given the privacy of voting booths, an attacker using such a card reader would be unlikely to be noticed. Given the ease with which an attacker can interact with legitimate smartcards, plus the weak password-based authentication scheme (see Section 3.3), an attacker could quickly gain enough insight to create homebrew voting cards, perhaps quickly enough to be able to use such homebrew cards during the same election day.

The only impediment to the mass production of homebrew smartcards is that each voting terminal will make sure that the smartcard has encoded in it the correct `m_ElectionKey`, `m_VCenter`, and `m_DLVersion` (see `DoVote()` in `BallotStation/Vote.cpp`). The `m_ElectionKey` and `m_DLVersion` are likely the same for all locations and, furthermore, for backward-compatibility purposes it is possible to use a card with `m_ElectionKey` and `m_DLVersion` undefined. The `m_VCenter` value could be learned on a per-location-basis by interacting with legitimate smartcards, from an insider, or from inferences based on the `m_VCenter` values observed at other polling locations.

It is worth pointing out that both the smartcards and readers supported by the code are available commercially over the Internet in small quantities. The smartcards, model number CLXSU004KC0, are available from CardLogix[4], where $33.50 buys ten cards. General purpose CyberFlex JavaCards from Schlumberger cost $110 for five cards[5]. Smartcard reader/writers are available in a variety of models for under $100 from many vendors.

In the following two subsections we illustrate what an attacker could accomplish using homebrew smartcards in voting terminals running the Diebold code.

[3] This, in an of itself, is an immediate red-flag. One of the biggest advantages of smartcards over classic magnetic-stripe cards is the smartcard's ability to perform cryptographic operations internally with physically protected keys. Since the smartcards in the Diebold system do not perform any cryptographic operations, they effectively provide no more security than traditional magnetic-stripe cards.

[4] `http://cardlogix.com/product_smart_select_most.asp`

[5] `http://www.scmegastore.com`

3.1.1 Multiple voting

In the Diebold system, a voter begins the voting process by inserting a smartcard into the voting terminal. Upon checking that the card is "active," the voting terminal collects the user's vote and then deactivates the user's card (the deactivation actually occurs by changing the card's type, which is stored as an 8-bit byte on the card, from `VOTER_CARD` (`0x01`) to `CANCELED_CARD` (`0x08`)). Since an adversary can make perfectly valid smartcards, the adversary could bring a stack of active cards to the voting booth. Doing so gives the adversary the ability to vote multiple times. More simply, instead of bringing multiple cards to the voting booth, the adversary could program a smartcard to ignore the voting terminal's deactivation command. Such an adversary could use one card to vote multiple times.

Will the adversary's multiple-votes be detected by the voting system? To answer this question, we must first consider what information is encoded on the voter cards on a per-voter basis. The only per-voter information is a "voter serial number" (`m_VoterSN` in the `CVoterInfo` class). Because of the way the Diebold system works, `m_VoterSN` is only recorded by the voting terminal if the voter decides *not* to place a vote (as noted in the comments in `TSElection/Results.cpp`, this field is recorded for uncounted votes for backward compatibility reasons). It is important to note that if a voter decides to cancel his or her vote, the voter will have the opportunity to vote again using that same card (and, after the vote has been cast, `m_VoterSN` will not be recorded).

Can the back-end tabulation system detect multiple-vote casting? If we assume the number of collected votes becomes greater than the number of people who showed up to vote, and if the polling locations keep accurate counts of the number of people who show up to vote, then the back-end system, if designed properly, should be able to detect the existence of counterfeit votes. However, because `m_VoterSN` is only stored for those who did not vote, there will be no way for the tabulating system to count the true number of voters or distinguish the real votes from the counterfeit votes. This would cast serious doubt on the validity of the election results. We point out, however, that we only analyzed the voting terminal's code; we do not know whether such checks are performed in the actual back-end tabulating system.

3.1.2 Administrator and ender cards

As noted in Section 2, in addition to the voter cards that users use when they vote, there are also administrator cards and ender cards. These cards have special purposes in this system. Namely, the administrator cards give the possessor the ability to access administrative functionality (namely, the administrative dialog `BallotStation/AdminDlg.cpp`), and both types of cards allow the possessor to end the election (hence the term "ender card").

Just as an adversary can manufacture his or her own voter cards, an adversary can manufacture his or her own administrator and ender cards (administrator cards have an easily-circumventable PIN, which we will discuss in Section 3.2). This attack is easiest if the attacker has knowledge of the Diebold code or can interact with a legitimate administrator or ender card. However, an attacker without knowledge of the inner-workings of the Diebold system and without the ability to interact directly with a legitimate administrator or ender card may have a difficult time producing a homebrew administrator or ender card since the attacker would not know what distinguishes an administrator or ender card from a normal voter card. (The distinction is that, for a voter card `m_CardType` is set to `0x01`, for an ender card `m_CardType` is set to `0x02`, and for an administrator card `m_CardType` is set to `0x04`.)

As one might expect, an adversary in possession of such illicit cards has further attack options against the Diebold system. Using a homebrew administrator card, a poll worker, who might not otherwise have access to the administrator functions of the Diebold system but who does have access to the voting machines before and after the elections, could gain access to the administrator controls. If a malicious voter entered an administrator or ender card into the voting device instead of the normal voter card, then the voter would be

able to terminate the election and, if the card is an administrator card, gain access to additional administrative controls.

The use of administrator or ender cards prior to the completion of the actual election represents an interesting denial-of-service attack. Once "ended," the voting terminal will no longer accept new voters (see `CVoteDlg::OnCardIn()`) until the terminal is somehow reset. Such an attack, if mounted simultaneously by multiple people, could shut down a polling place. If a polling place is in a precinct considered to favor one candidate over another, attacking that specific polling place could benefit the less-favored candidate. Even if the poll workers were later able to resurrect the systems, the attack might succeed in deterring a large number of potential voters from voting (e.g., if the attack was performed over the lunch hour). If such an attack was mounted, one might think the attackers would be identified and caught. We note that many governmental entities do not require identification to be presented by a voter, instead allowing for "provisional" ballots to be cast. By the time the poll workers realize that one of their voting terminals has been disabled, the perpetrator may have long-since left the scene.

3.2 Unprotected PINs

When a user enters an administrator card into a voting terminal, the voting terminal asks the user to enter a 4-digit PIN. If the correct PIN is entered, the user is given access to the administrative controls.

Upon looking more closely at this administrator authentication process, however, we see that there is a flaw with the way the PINs are verified. When the terminal and the smartcard first begin communicating, the PIN value stored on the card is sent in cleartext from the card to the voting terminal. Then, when the user enters the PIN into the terminal, it is compared with the PIN that the smartcard sent (`CPinDlg::OnOK()`). If these values are equal, the system accepts the PIN. Herein lies the flaw with this design: any person with a smartcard reader can easily extract the PIN from an administrator card. The adversary doesn't even need to fully understand the protocol between the terminal and the device: if the response from the card is n bytes long, the attacker who correctly guesses that the PIN is sent in the clear would only have to try $n-3$ possible PINs, rather than 10,000. This means that the PINs are easily circumventable. Of course, if the adversary knows the protocol between the card and the device, an adversary could just make his own administrator card, using any desired PIN (Section 3.1.2).

3.3 Terminal-to-card authentication

Let us now consider how the terminal authenticates to the card in more detail (note that this is different from the Administrator PIN; here the terminal is being authenticated rather than the user). The relevant code from `VoterCard/CLXSmartCard.cpp` is listed below. The code is slightly modified for illustrative purposes, but the developers' comments have been left intact.

```
SMC_ERROR CCLXSmartCard::Open(CCardReader* pReader)
{
  ... [removed code] ...

  // Now initiate access to the card
  // If failed to access the file then have unknown card
  if (SelectFile(0x3d40) != SMC_OK)
    st = SMC_UNKNOWNCARD;
  // Else if our password works then all done
  else if (Verify(0x80, 8, {0xed, 0x0a, 0xed, 0x0a, 0xed, 0x0a, 0xed, 0x0a})
    == SMC_OK)
    st = SMC_OK;
  // Else if manufactures password works then try to change password
  else if(Verify(0x80, 8, {0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08})
```

```
    == SMC_OK) {
    st = ChangeCode(8, {0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08},
                       8, {0xed, 0x0a, 0xed, 0x0a, 0xed, 0x0a, 0xed, 0x0a});
    // Else have a bad card
  } else
    st = SMC_BADCARD;
  return st;
}
```

In the above code, the `SelectFile(0x3d40)` command sends the bytes `0x00`, `0xA4`, `0x00`, `0x00`, `0x02`, `0x3D`, `0x40`, `0x00` to the smartcard in cleartext; this is the ISO 7816 smartcard command for selecting a file on the card (`0x3D40` in this case). If `passwd` is a sequence of 8 bytes, the `Verify(0x80, 8,passwd)` command sends the bytes `0x00`, `0x20 0x00`, `0x80`, `0x08`, `passwd[0]`, `passwd[1]`, `...`, `passwd[7]`, `0x00` to the smartcard in cleartext.

There are several issues with the above code. First, hard-coding passwords in C++ files is generally a poor design choice. We will discuss coding practices in more detail in Section 6, but we summarize some issues here. Hard-coding passwords into C++ files suggests a lack of key and password management. Furthermore, even if the developers assumed that the passwords would be manually changed and the software recompiled on a per-election basis, it would be very easy for someone to forget to change the constants in `VoterCard/CLXSmartCard.cpp`. (Recompiling on a per-election basis may also be a concern, since good software engineering practices would dictate additional testing and certification if the code were to be recompiled for each election.)

The above issues would only be a concern if the authentication method were otherwise secure. Unfortunately, it is not. Since the password is sent in the clear from the terminal to the card, an attacker who puts a fake card into the terminal and records the command from the terminal will be able to learn the password (and file name) and then re-use that password with real cards. An adversary with knowledge of this password could then create counterfeit voting cards. As we have already discussed (see Section 3.1.1), this can allow the adversary to cast multiple votes, among other attacks. Hence, the authentication of the voting terminal to the smartcards is insecure. We find this particularly surprising because modern smartcard designs allow cryptographic operations to be performed directly on the smartcard, making it possible to create systems that are not as easily vulnerable to security breaches.

Furthermore, note the control flow in the above code-snippet. If the password chosen by the designers of the system ("`\xED\x0A\xED\x0A\xED\x0A\xED\x0A`") does not work, then `CCLXSmartCard::Open()` uses the smartcard manufacturer's default password[6] of "`\x00\x01\x02\x03\x04\x05\x06\x07`." One issue with this is that it implies that sometimes the system is used with un-initialized smartcards. This means that an attacker might not even need to figure out the system's password in order to be able to authenticate to the cards. As we noted in Section 3.1, some smartcards allow a user to get a listing of all the files on a card. If the system uses such a card and also uses the manufacturer's default password of `\x00\x01\x02\x03\x04\x05\x06\x07`, then an attacker, even without any knowledge of the source code and without the ability to intercept the connection between a legitimate card and a voting terminal, but with access to a legitimate voter card, will still be able to learn enough about the smartcards to be able to create counterfeit voter cards.[7]

[6] Many smartcards are shipped with default passwords.

[7] Making homebrew cards this way is somewhat risky, as the attacker must make assumptions about the system. In particular, the attacker is assuming that his or her counterfeit cards would not be detected by the voting terminals. Without access to the source code, the attacker would never know, without testing, whether it was truly safe to attack a voting terminal.

4 Data storage

While the data stored internally on each voting terminal is not as accessible to an attacker as the voting system's smartcards, exploiting such information presents a powerful attack vector, especially for an election insider. In this section we outline the data storage available to each terminal and then detail how each distinct type of data is stored.

4.1 Data storage overview

Each voting terminal has two distinct types of internal data storage. A main (or system) storage area contains the terminal's operating system, program executables, static data files such as fonts, and system configuration information, as well as backup copies of dynamic data files such as the voting records and audit logs. Each terminal also contains a removable storage device that is used to store the primary copies of these dynamic data files. When the terminal is running a standard copy of Windows (e.g., Windows 2000) the removable storage area is the first floppy drive; when the terminal is running Windows CE the removable storage area is a removable storage card. Storing the dynamic data on two distinct devices is advantageous for both reliability and security: if either of the two storage mediums fails, data can still be recovered from the copy.

Unfortunately, under Windows CE, which we believe is used in commercial Diebold voting terminals, the existence of the removable storage device is not enforced properly. Unlike other versions of Windows, removable storage cards are mounted as subdirectories under CE. When the voting software wants to know if a storage card is inserted, it simply checks to see if the `Storage Card` subdirectory exists in the filesystem's root directory. While this is the default name for a mounted storage device, it is also a perfectly legitimate directory name for a directory in the main storage area. Thus, if such a directory exists, the terminal can be fooled into using the same storage device for all of the data.[8] This would reduce the amount of redundancy in the voting system and would increase the chances that a hardware fault could cause recorded votes to be lost.

4.2 System configuration

The majority of the system configuration information for each terminal is stored in the Windows registry under `HKEY_LOCAL_MACHINE\Software\GlobalElectionSystems\AccuVote-TS4` . This includes both identification information such as the terminal's serial number and more traditional configuration information such as the COM port that the smartcard reader is attached to. All of the configuration information is stored in the clear, without any form of integrity protection. Thus, all an adversary must do is modify the system registry to trick a given voting terminal into effectively impersonating any other voting terminal. It is unclear how the tallying authority would deal with results from two different voting terminals with the same voting ID — at the very least human intervention to resolve the conflict would probably be required.

The Federal Election Commission draft standard[9] requires each terminal to keep track of the total number of votes that have ever been cast on it — the "Protective Counter." This counter is used to provide yet another method for ensuring that the number of votes cast on each terminal is correct. However, as the following code from `Utilities/machine.cpp` shows, the counter is simply stored as an integer in the file `system.bin` in the terminal's system directory (error handling code has been removed for clarity):

[8] This situation can be easily corrected by checking for the `FILE_ATTRIBUTE_TEMPORARY` attribute on the directory as described in `http://msdn.microsoft.com/library/en-us/wcefiles/htm/_wcesdk_Accessing_Files_on_Other_Storage_Media.asp`

[9] `http://fecweb1.fec.gov/pages/vss/vss.html`

```
long GetProtectedCounter()
{
  DWORD protectedCounter = 0;
  CString filename = ::GetSysDir();
  filename += _T("system.bin");
  CFile file;
  file.Open(filename, CFile::modeRead | CFile::modeCreate |
                          CFile::modeNoTruncate);
  file.Read(&protectedCounter, sizeof(protectedCounter));
  file.Close();
  return protectedCounter;
}
```

By modifying this counter, an adversary could cast doubt on an election by creating a discrepancy between the number of votes cast on a given terminal and the number of votes that are tallied in the election. While the current method of implementing the counter is totally insecure, even a cryptographic checksum would not be enough to protect the counter; an adversary with the ability to modify and view the counter would still be able to roll it back to a previous state. In fact, the only solution that would work would be to implement the protective counter in a tamper-resistant hardware token, requiring modifications to the physical voting terminal hardware.

4.3 Ballot definition

The "ballot definition" for each election contains everything from the background color of the screen to the PPP username and password to use when reporting the results. This data is not encrypted or checksummed (cryptographically or otherwise) and so can be easily modified by any attacker with physical access to the file. While many attacks, such as changing the party affiliation of a candidate, would be noticed by some voters, many more subtle attacks are possible. By simply changing the order of the candidates as they appear in the ballot definition, the results file will change accordingly. However, the candidate information itself is not stored in the results file. The file merely tracks that candidate 1 got so many votes and candidate 2 got so many other votes. If an attacker reordered the candidates on the ballot definition, voters would unwittingly cast their ballots for the wrong candidate. As with denial-of-service attacks (see Section 3.1.2), ballot reordering attacks would be particularly effective in polling locations known to be heavily partisan.

Even without modifying the ballot definition, an attacker can gain almost enough information to impersonate the voting terminal to the back-end server. The terminal's voting center ID, PPP dial-in number, username, password and the IP address of the back-end server are all available in the clear (these are parsed into a `CElectionHeaderItem` in `TSElection\TSElectionObj.cpp`). Assuming an attacker is able to guess or create a voting terminal ID, he would be able to transmit fraudulent vote reports to the back-end server by dialing in from his own computer. While both the paper trail and data stored on legitimate terminals could be used to compensate for this attack after the fact, it could, at the very least, delay the election results. (The PPP number, username, password, and IP address of the back-end server are also stored in the registry `HKEY_LOCAL_MACHINE\Software\GlobalElectionSystems\AccuVote-TS4\TransferParams`. Since the ballot definition may be transported on portable memory cards or floppy disks, the ballot definition may perhaps be easier to obtain from this distribution media rather than from the voting terminal's internal data storage.)

We will return to some of these points in Section 5.1, where we show that modifying and viewing ballot definition files does not always require physical access to the terminals on which they are stored.

4.4 Votes and audit logs

Unlike the other data stored on the voting terminal, both the vote records and the audit logs are encrypted and checksummed before being written to the storage device. Unfortunately, neither the encrypting nor the checksumming is done securely.

All of the data on a storage device is encrypted using a single, hardcoded DES [NBS77] key:

```
#define DESKEY ((des_key*)"F2654hD4")
```

Note that this value is not a hex representation of a key. Instead, the bytes in the string "F2654hD4" are fed directly into the DES key scheduler. If the same binary is used on every voting terminal, an attacker with access to the source code, or even to a single binary image, could learn the key, and thus read and modify voting and auditing records. Even if proper key management were to be implemented, many problems would still remain. First, DES keys can be recovered by brute force in a very short time period [Gil98]. DES should be replaced with either triple-DES [Sch96] or, preferably, AES [DJ02]. Second, DES is being used in CBC mode which requires an initialization vector to ensure its security. The implementation here always uses zero for its IV. This is illustrated by the call to `DesCBCEncrypt` in `TSElection/RecordFile.cpp`; since the second to last argument is NULL, `DesCBCEncrypt` will use the all-zero IV.

```
DesCBCEncrypt((des_c_block*)tmp, (des_c_block*)record.m_Data, totalSize,
              DESKEY, NULL, DES_ENCRYPT);
```

This allows an attacker to mount a variety of cryptanalytic attacks on the data. To correctly implement CBC mode, a source of "strong" random numbers must be used to generate a fresh IV for each encryption [BDJR97]. Suitably strong random numbers can be derived from many different sources, ranging from custom hardware through observation of user behavior. (Jones reports that the vendor may have been aware of this design flaw in their code for several years [Jon01, Jon03]. We see no evidence that this design flaw was ever addressed.)

Before being encrypted, a 16-bit cyclic redundancy check (CRC) of the plaintext data is computed. This CRC is then stored along with the ciphertext in the file and verified whenever the data is decrypted and read. This process in handled by the `ReadRecord` and `WriteRecord` functions in `TSElection/RecordFile.cpp`. Since the CRC is an unkeyed, public function, it does not provide any real integrity for the data. In fact, by storing it in an unencrypted form, the purpose of encrypting the data in the first place (leaking no information about the contents of the plaintext) is undermined. A much more secure design would be to first encrypt the data to be stored and then to compute a keyed cryptographic checksum (such as HMAC-SHA1 [BCK96]) of the ciphertext. This cryptographic checksum could then be used to detect any tampering with the plaintexts. Note also that each entry has a timestamp, which will prevent the re-ordering, though not deletion, of records.

Each entry in a plaintext audit log is simply a timestamped, informational text string. At the time that the logging occurs, the log can also be printed to an attached printer. If the printer is unplugged, off, or malfunctioning, however, no record will be stored elsewhere to indicate that the failure occurred. The following code from `TSElection/Audit.cpp` demonstrates that the designers failed to consider these issues:

```
if (m_Print && print) {
CPrinter printer;
// If failed to open printer then just return.
CString name = ::GetPrinterPort();
if (name.Find(_T("\\")) != -1)
  name = GetParentDir(name) + _T("audit.log");
if (!printer.Open(name, ::GetPrintReverse(), FALSE))
  ::TSMessageBox(_T("Failed to open printer for logging"));
} else {
```

Do the printing...

}

If the cable attaching the printer to the terminal is exposed, an attacker could create discrepancies between the printed log and the log stored on the terminal by unplugging the printer (or, by simply cutting the cable).

An attacker's most likely target will be the voting records, themselves. Each voter's votes are stored as a bit array based on the ordering in the ballot definition file along with other information such as the precinct the voter was in, although no information that can be linked to a voter's identity is included. If the voter has chosen a write-in candidate, this information is also included as an ASCII string. An attacker given access to this file would be able to generate as many fake votes as he or she pleased, and such votes would be indistinguishable from the true votes cast on the terminal.

While the voter's identity is not stored with the votes, each vote is given a serial number. These serial numbers are generated by a linear congruential random number generator (LCG), seeded with static information about the election and voting terminal. No dynamic information, such as the current time, is used.

```
// LCG - Linear Conguential Generator - used to generate ballot serial numbers
// A psuedo-random-sequence generator
// (per Applied Cryptography, by Bruce Schneier, Wiley, 1996)
#define LCG_MULTIPLIER 1366
#define LCG_INCREMENTOR 150889
#define LCG_PERIOD 714025

static inline int lcgGenerator(int lastSN)
{
  return ::mod(((lastSN * LCG_MULTIPLIER) + LCG_INCREMENTOR), LCG_PERIOD);
}
```

While the code's authors apparently decided to use an LCG because it appeared in *Applied Cryptography* [Sch96], LCG's are far from secure. However, attacking this random number generator is unnecessary for determining the order in which votes were cast: each vote is written to the file sequentially. Thus, if an attacker is able to determine the order in which voters cast their ballots, the results file has a nice list, in the order in which voters used the terminal. A malevolent poll worker, for example, could surreptitiously track the order in which voters use the voting terminals. Later, in collaboration with other attackers who might intercept the poorly encrypted voting records, the exact voting record of each voter could be reconstructed. Physical access to the voting results may not even be necessary to acquire the voting records, if they are transmitted across the Internet.

5 Communicating with the outside world

The Diebold voting machines cannot work in isolation. They must be able to both receive a ballot definition file as input and report voting results as output. As described in Section 2, there are essentially two ways to load a voting terminal with an initial election configuration: via some removable media, such as a floppy disk, or over the Internet. In the latter case, the voting terminal could either be plugged directly into the Internet or could use a dial-up connection (the dial-up connection could be to a local ISP, or directly to the election authority's modem banks). After the election is over, election results are sent to a back-end post-processing server over the network (again, possibly through a dial-up connection).

Unfortunately, there are a number of attacks against this system that exploit the system's reliance on and communication with the outside world.

5.1 Tampering with ballot definitions

We first note that it is possible for an adversary to tamper with the voting terminals' ballot definition file (`election.edb`). If the voting terminals load the ballot definition from a floppy or removable storage card, then an adversary, such as a poll worker, could tamper with the contents of the floppy before inserting it into the voting terminal. On a potentially much larger scale, if the voting terminals download the ballot definition from the Internet, then an adversary could tamper with the ballot definition file en-route from the back-end server to the voting terminal. With respect to the latter, we point out that the adversary need not be an election insider; the adversary could, for example, be someone working at the local ISP. If a wireless network is used, anybody within radio range becomes a potential adversary. With high-gain antennas, the adversary can be sufficiently distant to have little risk of detection. If the adversary knows the structure of the ballot definition, then the adversary can intercept and modify the ballot definition while it is being transmitted. Even if the adversary does not know the precise structure of the ballot definition, many of the fields inside are easy to identify and change, including the candidates' names, which appear as plain ASCII text.[10]

Let us now consider some example attacks that make use of modifying the ballot definition file. Because no cryptographic techniques are in place to guard the integrity of the ballot definition file, an attacker could add, remove, or change issues on the ballot, and thereby confuse the result of the election.

In the system, different voters can be presented with different ballots depending on their party affiliations (see `CBallotRelSet::Open()`, which adds different issues to the ballot depending on the voter's `m_VGroup1` and `m_VGroup2` `CVoterInfo` fields). If an attacker changes the party affiliations of the candidates, then he may succeed in forcing the voters to view and vote on erroneous ballots. Even in municipalities that use the same ballot for all voters, a common option in voting systems is to allow a voter to select all the candidates from a given political party. Voters may not notice if candidates have incorrect party affiliations listed next to their names, and by choosing to vote a straight ticket, would end up casting ballots for undesirable candidates.

As an example of what might happen if the party affiliations were listed incorrectly, we note that, according to a news story[11], in the 2000 New Mexico presidential election, over 65,000 votes were incorrectly counted because a worker accidentally had the party affiliations wrong. (We are not claiming, however, that those affiliations were maliciously assigned incorrectly. Nor are we implying that this had an effect on the results of the election.)

Likewise, an attacker who can change the ballot definition could also change the ordering of the candidates running for a particular office. Since, at the end of the election, the results are uploaded to the server in the order that they appear in the the ballot definition file, and since the server will believe that the results appear in their original order, this attack could also succeed in swapping the votes between parties in a predominantly partisan precinct. This ballot reordering attack is also discussed in more detail in Section 4.3.

5.2 Preventing the start of an election

Suppose that the election officials are planning to download the configuration files over the Internet and that they are running late and do not have much time before the election starts to distribute ballot definitions manually (i.e., they might not have enough time to distribute physical media with the ballot definition files from central office to every voting precinct). In such a situation, an adversary could mount a traditional

[10] The relevant sections of code are as follows: `CTransferElecDlg::OnTransfer()` invokes `CTSElectionDoc::CreateEDB()`, which reads the data from a `CDL2Archive`. The way the code works, `CDL2Archive` reads and writes to a `CBufferedSocketFile`. Returning to `CTSElectionDoc::CreateEDB()`, we see that it invokes `CTSElectionDB::Create()`, which subsequently invokes `CTSElectionFile::Save()`. The functions called in `CTSElectionFile::Save()` read data, such as strings, from the `CDL2Archive`.

[11] `http://www.gcn.com/vol19_no33/news/3307-1.html`

Internet denial-of-service attack against the election management's server and thereby prevent the voting terminals from acquiring their ballot definitions before the start of the election. To mount such an attack effectively, the adversary would ideally need to know the topology of the system's network, and the name of the server(s) supplying the ballot definition file.[12] If a fair number of people from a certain demographic plan to vote early in the morning, then this could impact the results of the election.

Of course, we acknowledge that there are other ways to postpone the start of an election at a voting location that do not depend on the use of this system (e.g., flat tires for all poll workers for a given precinct). Unlike such traditional attacks, however, the network-based attack (1) is relatively easy for anyone with knowledge of the election system's network topology to accomplish; (2) this attack can be performed on a very large scale, as the central distribution point(s) for ballot definitions becomes an effective single point of failure; and (3) the attacker can be physically located anywhere in the Internet-connected world, complicating efforts to apprehend the attacker. Such attacks could prevent or delay the start of an election at all voting locations in a state. We note that this attack is not restricted to the system we analyzed; it is applicable to any system that downloads its ballot definition files using the Internet.

5.3 Tampering with election results

Just as it is possible for an adversary to tamper with the downloading of the ballot definition file (Section 5.1), it is also possible for an adversary to tamper with the uploading of the election results. To make this task even easier for the adversary, we note that although the election results are stored "encrypted" on the voting devices (Section 4.4), the results are sent from the voting devices to the back-end server over an unauthenticated and unencrypted channel. In particular, `CTransferResultsDlg::OnTransfer()` writes ballot results to an instance of `CDL2Archive`, which then writes the votes in cleartext to a socket without any cryptographic checksum.

Sending election results in this way over the Internet is a bad idea. Nothing prevents an attacker with access to the network traffic, such as workers at a local ISP, from modifying the data in transit. Such an attacker could, for example, decrease one candidates vote count by n and increase the another candidate's count by n. Of course, to introduce controlled changes to the votes, the attacker would require some knowledge of the structure of the messages sent from the voting terminals to the back-end server. If the voting terminals use a modem connection directly to the tabulating authority's network, rather than the Internet, then the risk of such an attack is less, although still not inconsequential. A sophisticated adversary (or employee of the local phone company) could tap the phone line and intercept the communication. All of these adversaries could be easily defeated by properly using standard encryption suites like SSL/TLS, used throughout the World Wide Web for e-commerce security. We are puzzled why such a widely accepted and studied technology is not used by the voting terminals to safely communicate across potentially hostile networks.

5.4 Attacking the voting terminals directly

In some configurations, where the voting terminals are directly connected to the Internet, it may be possible for an adversary to attack them directly, perhaps using an operating system exploit or buffer overflow attack of some kind. Ideally the voting devices and their associated firewalls would be configured to accept no incoming connections [CBR03]. This concern would apply to any voting terminal, from any vendor, with a direct Internet connection.

[12] Knowledge of the specific servers is unnecessary for a large scale distributed denial of service attack. An attacker simply needs to correctly guess that the ballot definition's file server is on a specific network (e.g., at the voting system's vendor or in the municipality's government).

6 Software engineering

When creating a secure system, getting the design right is only part of the battle. The design must then be securely implemented. We now examine the coding practices and implementation style used to create the voting device. This type of analysis can offer insights into future versions of the code. For example, if a current implementation has followed good implementation practices but is simply incomplete, one would be more inclined to believe that future, more complete versions of the code would be of a similar high quality. Of course, the opposite is also true, perhaps even more so: it is very difficult to produce a secure system by building on an insecure foundation.

Of course, reading the source code to a product gives only an incomplete view into the actions and intentions of the developers who created that code. Regardless, we can see the overall software design, we can read the comments in the code, and thanks to the CVS repository, we can even look at earlier versions of the code and read the developers' commentary as they committed their changes to the archive.

6.1 Code Legacy

Inside `cvs.tar` we found multiple CVS archives. Two of the archives, `AccuTouch` and `AVTSCE` implement full voting terminals. The `AccuTouch` code dates to around 2000 and is copyrighted by "Global Election Systems, Inc." while the `AVTSCE` code dates to mid-2002 and is copyrighted by "Diebold Election Systems, Inc." (The CVS logs show that the copyright notice was updated on February 26, 2002.) Many files are nearly identical between the two systems and the overall design appears very similar. Indeed, Diebold acquired Global Election Systems in September, 2001.[13] Some of the code, such as the functions to compute CRCs and DES, dates back to 1996, when Global Election Systems was called "I-Mark Systems."

This legacy is apparent in the code itself as there are portions of the `AVTSCE` code, including entire classes, that are either simply not used or removed through the use of `#ifdef` statements. Many of these functions are either incomplete or, worse, do not perform the function that they imply as is the case with `CompareFiles` in `Utilities/FileUtil.cpp`:

```
BOOL CompareFiles(const CString& file1, const CString& file2)
{
  /* XXX use a CRC or something similar */
  BOOL exists1, exists2;
  HANDLE hFind;
  WIN32_FIND_DATA fd1, fd2;

  exists1 = ((hFind = ::FindFirstFile(file1, &fd1)) != INVALID_HANDLE_VALUE);
  ::FindClose(hFind);

  exists2 = ((hFind = ::FindFirstFile(file2, &fd2)) != INVALID_HANDLE_VALUE);
  ::FindClose(hFind);

  return (exists1 && exists2 && fd1.nFileSizeLow == fd2.nFileSizeLow);
}
```

Currently the code will declare any two files to be the same that have the same size. The author's comment to use a CRC doesn't make much sense, as a byte-by-byte comparison would be more efficient. If this code were ever used, its inaccuracies could lead to wide variety of subsequent errors.

While most of the preprocessor directives that remove code correctly use `#if 0` as their condition, some use `#ifdef XXX`. There is no reason that a later programmer should realize that defining `XXX` will cause blocks of code to be reincluded in the system (causing unpredictable results, at best). We also noticed

[13] http://dallas.bizjournals.com/dallas/stories/2001/09/10/daily2.html

`#ifdef LOUISIANA` in the code. Prudent software engineering would recommend a single implementation of the voting software, where individual states or municipalities could have their desired custom features expressed in configuration files.

6.2 Coding style

While the system is implemented in an unsafe language (C++), the code reflects an awareness of avoiding such common hazards as buffer overflows. Most string operations already use their safe equivalents, and there are comments reminding the developers to change others (e.g., `should really use _snprintf`). While we are not prepared to claim that there are no buffer overflows in the current code, there are at the very least no glaringly obvious ones. Of course, a better solution would have been to write the entire system in a safe language, such as Java or C#.

The core concepts of object oriented programming such as encapsulation are well represented, though in some places C++'s non-typesafe nature is exploited with casts that could conceivably fail. This could cause problems in the future as these locations are not well documented.

Overall, the code is rather unevenly commented. While most files have a description of their overall function, the meanings of individual functions, their arguments, and the algorithms within are more often than not undocumented. An extreme example of a complex but completely undocumented function is the `CBallotRelSet::Open` function from `TSElection/TSElectionSet.cpp`:

```
void CBallotRelSet::Open(const CDistrict* district, const CBaseunit* baseunit,
                                    const CVGroup* vgroup1, const CVGroup* vgroup2)
{
   ASSERT(m_pDB != NULL);
   ASSERT(m_pDB->IsOpen());
   ASSERT(GetSize() == 0);
   ASSERT(district != NULL);
   ASSERT(baseunit != NULL);

   if (district->KeyId() == -1) {
      Open(baseunit, vgroup1);
   } else {
      const CDistrictItem* pDistrictItem = m_pDB->Find(*district);
      if (pDistrictItem != NULL) {
         const CBaseunitKeyTable& baseunitTable = pDistrictItem->m_BaseunitKeyTable;
         int count = baseunitTable.GetSize();
         for (int i = 0; i < count; i++) {
            const CBaseunit& curBaseunit = baseunitTable.GetAt(i);
            if (baseunit->KeyId() == -1 || *baseunit == curBaseunit) {
               const CBallotRelationshipItem* pBalRelItem = NULL;
               while ((pBalRelItem = m_pDB->FindNextBalRel(curBaseunit, pBalRelItem))){
                  if (!vgroup1 || vgroup1->KeyId() == -1 ||
                    (*vgroup1 == pBalRelItem->m_VGroup1 && !vgroup2) ||
                    (vgroup2 && *vgroup2 == pBalRelItem->m_VGroup2 &&
                       *vgroup1 == pBalRelItem->m_VGroup1))
                     Add(pBalRelItem);
               }
            }
         }
         m_CurIndex = 0;
         m_Open = TRUE;
      }
   }
}
```

Nothing about this code makes its purpose readily apparent. Certainly, it has two nested loops and is doing all kinds of comparisons. Beyond that, most readers of the code would need to invest significant time to learn the meaning of the various names shown here.

6.3 Coding process

An important point to consider is how code is added to the system. From the CVS logs, we can see that most code updates are in response to specific bugs that needed to be fixed. There are numerous authors who have committed changes to the CVS tree, and the only evidence that we have found that the code undergoes any sort of review process comes from a single log comment: "Modify code to avoid multiple exit points to meet Wyle requirements." This could refer to Wyle Laboratories whose website claims that they provide all manner of testing services.[14]

There are also pieces of the voting system that come from third parties. Most obviously is the operating system, either Windows 2000 or Windows CE. Both of these OSes have had numerous security vulnerabilities and their source code is not available for examination to help rule out the possibility of future attacks. Besides the operating system, an audio library called "fmod" is used.[15] While the source to fmod is available with commercial licenses, unless the code is fully audited there is no proof that fmod itself does not contain a backdoor.

Due to the lack of comments, the legacy nature of the code, and the use of third-party code and operating systems, we believe that any sort of comprehensive, top-to-bottom code review would be nearly impossible. Not only does this increase the chances that bugs exist in the code, but it also implies that any of the coders could insert a malicious backdoor into the system. The current design deficiencies provide enough other attack vectors that such an explicit backdoor is not required to successfully attack the system. Regardless, even if the design problems are eventually rectified, the problems with the coding process may well remain intact.

6.4 Code completeness and correctness

While the code we studied implements a full system, the implementors have included extensive comments on the changes that would be necessary before the system should be considered complete. It is unclear whether the programmers actually intended to go back and remedy all of these issues as many of the comments existed, unchanged, for months, while other modifications took place around them. It is also unclear whether later version of AVTSCE were subsequently created. (Modification dates and locations are easily visible from the CVS logs.) These comments come in a number of varieties. For illustrative purposes, we have chosen to show a few such comments from the subsystem that plays audio prompts to visually-impaired voters.

- Notes on code reorganization:
  ```
  /* Okay, I don't like this one bit.  Its really tough to tell
  where m_AudioPlayer should live.  [...]  A reorganization might be
  in order here.  */
  ```
- Notes on parts of code that need cleaning up:
  ```
  /* This is a bit of a hack for now.  [...]  Calling from the timer
  message appears to work.  Solution is to always do a 1ms wait
  between audio clips.  */
  ```

[14] http://www.wylelabs.com/te.html
[15] http://www.fmod.org/

- Notes on bugs that need fixing:
  ```
  /* need to work on exception *caused by audio*.  I think they will
  currently result in double-fault.  */
  ```

There are, however, no comments that would suggest that the design will radically change from a security perspective. None of the security issues that have been discussed in this paper are pointed out or marked for correction. In fact, the only evidence at all that a redesign might at one point have been considered comes from outside the code: the Crypto++ library[16] is included in another CVS archive in `cvs.tar`. However, the library was added in September 2000 and was never used or updated. We infer that one of the developers may have thought that improving the cryptography would be useful, but then got distracted with other business.

7 Conclusions

Using publicly available source code, we performed an analysis of a voting machine. This code was apparently developed by a company that sells to states and other municipalities that use them in real elections. We found significant security flaws: voters can trivially cast multiple ballots with no built-in traceability, administrative functions can be performed by regular voters, and the threats posed by insiders such as poll workers, software developers, and even janitors, is even greater. Based on our analysis of the development environment, including change logs and comments, we believe that an appropriate level of programming discipline for a project such as this was not maintained. In fact, there appears to have been little quality control in the process.

For quite some time, voting equipment vendors have maintained that their systems are secure, and that the closed-source nature makes them even more secure. Our glimpse into the code of such a system reveals that there is little difference in the way code is developed for voting machines relative to other commercial endeavors. In fact, we believe that an open process would result in more careful development, as more scientists, software engineers, political activists, and others who value their democracy would be paying attention to the quality of the software that is used for their elections. (Of course, open source would not solve all of the problems with electronic elections. It is still important to verify somehow that the binaries running in the machine correspond to the source code and that the compilers used on the source code are non-malicious. However, open source is a good start.) Such open design processes have proven successful in projects ranging from very focused efforts, such as specifying the Advanced Encryption Standard (AES) [NBB+00], through very large and complex systems such as maintaining the Linux operating system.

Alternatively, security models such as the voter-verified audit trail allow for electronic voting systems that produce a paper trail that can be seen and verified by a voter. In such a system, the correctness burden on the voting terminal's code is less extreme because voters can see and verify a physical object that embodies their vote. Even if, for whatever reason, the machines cannot name the winner of an election, then the paper ballots can be recounted, either mechanically or manually, to gain progressively more accurate election results.

The model where individual vendors write proprietary code to run our elections appears to be unreliable, and if we do not change the process of designing our voting systems, we will have no confidence that our election results will reflect the will of the electorate. We owe it to ourselves and to our future to have robust, well-designed election systems to preserve the bedrock of our democracy.

[16] `http://www.eskimo.com/~weidai/cryptlib.html`

Acknowledgments

We thank Cindy Cohn, David Dill, Badri Natarajan, Jason Schultz, David Wagner, and Richard Wiebe for their suggestions and advice.

References

[BCK96] M. Bellare, R. Canetti, and H. Krawczyk. Keying hash functions for message authentication. In *Advances in Cryptology: Proceedings of CRYPTO '96*, pages 1–15. Springer-Verlag, 1996.

[BDJR97] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A concrete security treatment of symmetric encryption. In *Proceedings of the 38th Annual Symposium on Foundations of Computer Science*, pages 394–403. IEEE Computer Society Press, 1997.

[Cal00] California Internet Voting Task Force. *A report on the feasiblility of Internet voting*, January 2000. `http://www.ss.ca.gov/executive/ivote/`.

[Cal01] *Voting: What Is; What Could be*, July 2001. `http://www.vote.caltech.edu/Reports/`.

[CBR03] W. R. Cheswick, S. M. Bellovin, and A. D. Rubin. *Firewalls and Internet Security; Repelling the Wily Hacker*. Addison-Wesley, Reading, MA, 2003.

[Die03] Diebold Election Systems. `AVTSCE/` source tree, 2003. Available in `http://users.actrix.co.nz/dolly/Vol2/cvs.tar`.

[DJ02] J. Daemen and V. Jijmen. *The Design of Rijndael: AES–The Advanced Encryption Standard*. Springer, 2002.

[DMNW03] D. L. Dill, R. Mercuri, P. G. Neumann, and D. S. Wallach. *Frequently Asked Questions about DRE Voting Systems*, February 2003. `http://www.verifiedvoting.org/drefaq.asp`.

[Gil98] J. Gilmore, editor. *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design*. O'Reilly, July 1998.

[Har03] B. Harris. *Black Box Voting: Vote Tampering in the 21st Century*. Elon House/Plan Nine, July 2003.

[Jon01] D. W. Jones. *Problems with Voting Systems and the Applicable Standards*, May 2001. Testimony before the U.S. House of Representatives' Committee on Science, `http://www.cs.uiowa.edu/~jones/voting/congress.html`.

[Jon03] D. W. Jones. *The Case of the Diebold FTP Site*, July 2003. `http://www.cs.uiowa.edu/~jones/voting/dieboldftp.html`.

[Ker83] A. Kerckhoffs. *La Cryptographie Militaire*. Libraire Militaire de L. Baudoin & Cie, Paris, 1883.

[Mer00] R. Mercuri. *Electronic Vote Tabulation Checks and Balances*. PhD thesis, University of Pennsylvania, Philadelphia, PA, October 2000.

[Nat01] National Science Foundation. *Report on the National Workshop on Internet Voting: Issues and Research AGenda*, March 2001. `http://news.findlaw.com/cnn/docs/voting/nsfe-voterprt.pdf`.

[NBB+00] J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, and E. Roback. *Report on the Development of the Advanced Encryption Standard (AES)*, October 2000.

[NBS77] NBS. Data encryption standard, January 1977. Federal Information Processing Standards Publication 46.

[Rub02] A. D. Rubin. Security considerations for remote electronic voting. *Communications of the ACM*, 45(12):39–44, December 2002. `http://avirubin.com/e-voting.security.html`.

[Sch96] B. Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, New York, second edition, 1996.

[Sch00] B. Schneier. *Secrets and Lies*. John Wiley & Sons, New York, 2000.

Congress of the United States
Washington, DC 20515

March 3, 2004

Dear Colleague:

As the principal authors of the Help America Vote Act (Public Law 107-252) (HAVA), signed into law by President Bush on October 29, 2002, we feel compelled to express our concerns about recent legislative efforts that promise enhanced electronic voting system security. Various proposals have been introduced in the House and Senate, but a common feature of these bills is they would amend HAVA to require that all voting systems, including electronic and computer-based systems, produce or accommodate a "voter verified paper record." Not only are such proposals premature, but they would undermine essential HAVA provisions, such as the disability and language minority access requirements, and could result in more, rather than less, voter disenfranchisement and error.

We are certainly aware of the alleged concerns that have been raised in recent months regarding security issues associated with computer-based voting systems and technologies, especially Direct Recording Electronic (DRE) voting systems. These concerns are neither new nor unanticipated by HAVA. To address security-related issues, HAVA creates a Technical Guidelines Development Committee, chaired by the Director of the National Institute of Standards and Technology (NIST), to assist the new Election Assistance Commission (EAC) in developing guidelines and standards to ensure the reliability of the computer technologies being employed in voting systems. These standards will focus not only on the security of computer and network hardware and software and data storage, but also on the detection and prevention of fraud and the protection of voter privacy. Additionally, HAVA provides that the testing and certification of voting system hardware and software must take place in accredited laboratories. NIST initiated this process with a two-day public conference this past December, 2003.

The goal of HAVA is to ensure that every eligible American has an equal opportunity to cast a vote and have that vote counted. HAVA does not mandate the use of DRE systems. It does require, however, that voting systems be enhanced to avoid the errors and accessibility problems associated with antiquated systems, such as punch cards. Computer-based voting systems have a demonstrated track record of achieving this goal, particularly for persons with disabilities. While there are risks associated with any technology, the solution is not to rush to judgment by returning to flawed systems. Rather, the answer is to allow the Commission, together with the active input of election officials, computer experts, and civil rights groups representing voter interests, to develop standards for ensuring the security of all voting systems, as required under HAVA.

The proposals mandating a voter-verified paper record would essentially take the most advanced generations of election technologies and systems available and reduce

PRINTED ON RECYCLED PAPER

them to little more than ballot printers. While such an approach may be one way to address DRE security issues, it would, if adopted, likely give rise to numerous adverse unintended consequences. Most importantly, the proposals requiring a voter-verified paper record would force voters with disabilities to go back to using ballots that provide neither privacy nor independence, thereby subverting a hallmark of the HAVA legislation. There must be voter confidence in the accuracy of an electronic tally. However, the current proposals would do nothing to ensure greater trust in vote tabulations but would be guaranteed to impose steep costs on States and localities and introduce new complications into the voting process.

Questions regarding voting systems security, as well as many others, need to be examined by the entity responsible for doing so under existing law, the Election Assistance Commission, before Congress begins imposing new requirements, just months before the 2004 presidential and congressional elections, that have not been fully considered. The security of voting technology is a non-partisan issue. We encourage you to allow HAVA to be implemented as enacted and provide those who are charged with ensuring the security of voting systems the time and flexibility needed to get the job done effectively.

Sincerely,

ROBERT W. NEY

STENY HOYER

MITCH MCCONNELL

CHRISTOPHER J. DODD

Election Systems & Software Electronic Voting Systems: Accurate, Secure, Reliable, and Accessible

January 20, 2004

By ES&S, the nation's leading provider of election solutions

Introduction

The Help America Vote Act (HAVA) of 2002 allows for major improvements in the nation's elections systems. Among other things, it will provide much needed funding to states and localities to replace outdated punch card and lever voting systems with new voting technology. These new systems provide a number of advantages, including improved security and reliability, faster tabulation, multiple language capabilities, and broader voting accessibility to the disabled population.

Clearly, this is an exciting time for the American electorate, as well as state and county election administrators. But, because of the newness of today's voting technology, some have raised questions about the security and reliability of direct recording electronic (DRE) systems. Based on our experience supporting thousands of successful elections every year and the assessments of others, we can say with certainty that the DRE equipment used today by Election Systems & Software (ES&S) is secure. In fact, voting technology has never been more accurate, more reliable, or easier to use.

At ES&S, we recognize the incredible responsibility we have to voters around the world, so we hold ourselves to a higher standard. We're proud of and take seriously our role in the democratic process. Maintaining voter confidence – and enhancing the voting experience – is at the core of our mission as a company.

Today's Proven Technology

While current election technology is more high-tech than ever before, our core values at ES&S have not changed one bit over the last 30 years. We provide accurate, secure, reliable, and accessible voting systems that result in full and fair elections. To that end, we have continuously developed hardware and software to meet the unique needs of each jurisdiction as well as the special needs of the elderly and disabled, from improved voter registration mechanisms to multi- lingual and audio ballots.

HAVA, which provides significant funding for local jurisdictions to upgrade their voting equipment, will go a long way toward making available to people across the country the innovative and easy-to-use technology ES&S has pioneered. Our iVotronic™ election equipment – today's proven, secure direct recording electronic voting technology, also known as touch screen equipment – makes it easier for votes to be both cast and tabulated.

Our Systems Are Secure

As ES&S continues to develop new technology and make existing voting options even better, the principles of security, accuracy, and reliability are at the forefront of what we do, every day. Comprehensive checks and balances are integrated throughout the voting process to help ensure the security of the elections we serve. Complementary and integrated security safeguards are inserted at every step of the voting process – before, during, and after an election – from the development and design of DRE hardware and software to specific processes and procedures that must be followed by local election officials to ensure accurate and reliable voting and tabulation.

It is important to note that today, all election equipment in the United States is tested by independent test authorities (ITAs). The ITAs ensure that the equipment meets or exceeds the requirements of the Federal Elections Commission's voting standards. The ITA testing and certification processes are rigorous, ensuring that the systems meet federal and state requirements on a number of fronts – including source code, hardware, software, environmental, functional, logic, and reliability. (The testing standards are available at www.fec.gov)

And, although the government sets common standards that govern equipment used industry-wide, there are a number of unique security safeguards that set apart ES&S's DRE voting technology from the rest. Among other things:

• The closed system and unique personal electronic ballot (PEB) used by ES&S are not open to either wireless or wire-based systems, and do not allow Internet connections, direct phone line connections, or direct network connections. Therefore, the system is protected from any kind of outside manipulation.

• The PEB is designed as an integrated part of the system. It is not accessible without specific read/write mechanisms supplied by ES&S to only the election administrators of the system.

• The iVotronic has three physically independent memory chips that store the electronic ballot data. The data from all three memories are checked for verification with each other prior to allowing a vote or the casting of a vote to ensure no vote is allowed or cast if there is an error.

• In addition to these unique features, the iVotronic employs a number of common failsafe features such as election and poll place-specific password protection, public and protective ballot counters, date and time stamps for audit log events, as well as physical seals and secure procedural processes to prevent the chance of mistakes or election fraud.

Election Process Ensures Security

Despite these numerous protections, the human factor must be taken into consideration. As with automobiles, for example, safety does not rely solely on the way the vehicle is built. Safety also depends on the way the car is driven, the way other drivers operate their vehicles, and on the laws that govern vehicle design and operation. While the way the car is built is very important, it is not the only factor. Likewise, regardless of the security safeguards that are employed in the election industry election hardware systems, there may be those who purposefully try to find ways to disrupt or add fraud to the system. To minimize that factor, voting officials must be highly trained and educated about the voting systems, and they must be vigilant about taking the steps that we outline to help ensure overall election security. It is the combination of the security features built into the systems with election administrators using proven election processes before, during, and after the election that results in a secure, reliable, accurate election.

Tomorrow's Technology Today

For more than 30 years, ES&S has been responsive to the election industry, local election administration, and election governing bodies. Over those years, we have embraced change and made investments needed to support the demands within the election industry. Although current DRE technology provides a proven, accurate and reliable vote count, some are calling for DRE systems to include the capability to print a voter verification paper receipt. There are many issues surrounding the question of paper receipts. And, though ES&S has assumed a leadership position in this discussion by developing prototype technology, it is policymakers who must weigh the pros and cons and choose a direction. When a decision is made to move forward with voter verification paper receipts and standards are in place, ES&S stands ready to support implementation. After all, ES&S is in the business of providing secure, accurate and reliable election systems that guarantee full public and voter confidence. At the same time, we would like to offer the following thoughts to be considered as the election industry evaluates the voter verifiable paper receipt.

- The current systems are fully auditable and secure. Accuracy can be verified for each terminal through current electronic ballot records already stored within the terminals and with random audits of polling locations. Current election systems review, testing practices, and procedures would detect any rogue, malicious, or fraudulent code, if present, within a DRE.

- Managing the voter verification paper receipt raises some needs worth considering. Among these needs are physical paper handling and storage administration, mechanical printer maintenance, increased costs in both the hardware and election logistics, as well as additional processes and procedures required for both the voter and the poll workers.

- To be prepared, ES&S' current DRE technology has been built with the ability to support a printer. Prototypes have been designed and demonstrated across the country.

With clarity from election offices and governing bodies on specific standards, ES&S is prepared to turn the prototype into a certified, production ready unit. We would welcome the opportunity to visit with any state or county representative to demonstrate our working prototype.

Proven Experience

With more than three decades of experience in providing safe and secure elections systems, Election Systems & Software (ES&S) has more direct expertise than anyone in the industry. Our entire business is focused on delivering full and fair elections – from innovating and building the hardware that's used in vote tabulation, to developing the software used to create and manage voter registration databases, to providing the support services that help make election night run smoothly. In the past decade, ES&S has handled more than 30,000 elections, and in the 2000 U.S. general election alone, ES&S systems counted more than 100 million ballots. In fact, there is hardly a day in the calendar year when we are not involved in an election in at least one jurisdiction around the country.

Asian Pacific American Legal Center
1145 Wilshire Blvd. 2nd floor
Los Angeles, CA 90017
213-977-7500

June 27, 2003

Secretary of State Kevin Shelley
Elections Division
1500 11th Street
Sacramento, CA 95814

Via fax: (916) 653-3214

Dear Secretary of State Kevin Shelley,

Re: Paper Trails and Voting Technology

On behalf of the Asian Pacific American Legal Center (APALC), I am writing to express opposition to a mandatory requirement for voting systems to have a voter-verifiable paper trail.

As you know, APALC has been conducting regular poll monitoring of major elections in Southern California for the last decade, to ensure LA and Orange County are complying with Section 203 of the Voting Rights Act. Providing meaningful access to the voting process for our Asian American communities where for many, English may not be their first language, is a continuing challenge for local election officials. We continue to see problems with voters unable to communicate with poll workers, not receiving their translated sample ballots or other materials on time, and arriving at poll sites with no translated materials.

Based on observations of several elections where LA County has offered touch screen voting, APALC has substantial evidence that touch screen voting and similar Direct Record Electronic (DRE) technologies will remove current language barriers. As you well know, DREs afford users the option of choosing to vote in the language of their choice, and to see their entire ballot in that language. DREs make language assistance available at ALL poll sites with DREs, not just select ones, as is the case now. Most importantly, in several past elections, APALC has observed voters needing language assistance of all ages and backgrounds use DREs with surprising ease and receptivity – even seniors who have never used an ATM before. Clearly, DREs also afford other advantages, including lower error rates for minority and all voters, accessibility to voters with disabilities, and a user-friendly platform for alternative voting systems

APALC is concerned that a mandatory voter-verified paper trail requirement may prevent election officials from switching to DRE technology. We have seen major metropolitan areas that have large language minority and other populations – such as San Francisco and Sacramento – hampered in this paper trail debate from purchasing the only technology that will improve voter participation. "Opti-scan," "Ink-a-vote," "Broken arrow" and other paper-based systems have proven to be very difficult or impossible for new voters and voters with special needs to understand or use without spoiling their ballot. Yet, these are the technologies that counties are choosing because of the fears raised from the Florida elections. Ironically, Florida had voter-

verifiable paper ballots – a fact that did nothing to improve voter confidence or the accuracy of the vote count.

There is much misinformation about the audit capacity and safeguards available with DREs. Many people do not know that DREs have the capacity and are being equipped with an internal paper trail and multiple methods of backing up the data. There is also misinformation about DREs being connected to a live phone line that might allow hacking. As such, the fears expressed are largely unfounded. We urge you to address the need for voter confidence with a public awareness campaign – not a voter-verified paper trail requirement.

We request that the Secretary of State engage in additional research and discussions with vendors to allow for additional ballot security measures to be developed and understood. While we support instituting various safeguards in all voting systems to ensure against errors and tampering, we urge you not to institute a mandatory voter-verified paper trail requirement.

Sincerely,

Kathay Feng, Esq.
Voting Rights, Unit Director
Asian Pacific American Legal Center

DIEBOLD®
ELECTION SYSTEMS

July 29, 2003

Summary technical analysis of recent voting system report

A prior version of Diebold Election Systems' touch screen software was analyzed on a device upon which it was never intended to run, using an operating system for which it was not designed, and with minimal knowledge of the overall structures and processes in which the terminal software is embedded. In addition, many of the weaknesses attributed to the operating system on which the software was tested are inapplicable to the embedded operating system actually used by Diebold Election Systems. As a result, many of the conclusions drawn by the researchers are inaccurate or incomplete with respect to the security of this particular element of the voting system.

Incorrect operating system and hardware used

The researchers installed and analyzed a prior version of the AccuVote®-TS software on a typical personal computer, on which a generally available Microsoft® operating system was installed. This personal computer on which the software was analyzed also had an Internet or continuous modem connection, a keyboard, and disk drives. The exploitation of many of the weaknesses attributed to Diebold Election Systems' software resulted from this configuration, which does not exist when the software is used in a Diebold Election Systems voting terminal.

Terminals are never connected to Internet

The researchers indicate that in order for last minute or stealth changes to be downloaded to a voting terminal, a continuous or unmonitored Internet or modem connection would be necessary. The installation and operating procedures used by Diebold Election Systems include neither. Diebold Election Systems does not connect its voting terminals to the Internet. A brief secure connection to an isolated server, typically in the same room as the designated terminal, is used to program memory cards. Once the memory cards are programmed, the server connection is severed. The software is loaded onto the voting terminals from the memory cards, the software is tested, the terminal is locked and a tamper-indicating device affixed.

Terminal design prevents easy access

Unlike the personal computer on which the analysis was performed, the voting terminal does not have a standard keyboard or disk drives, and the redundant memory is physically locked into the machine. This makes unavailable the easy access required to accomplish some of the other security breaches that have been suggested by the

researchers. For example, without access to drives or a keyboard, an a changing registry entries or files would not be easily accomplished.

Layers of security prevent creating voting cards

Similarly, unlike the personal computer on which the analysis was perfo reader is an integrated portion of the voting terminal. This configuration realistically impossible the wire tapping necessary to capture the data re a "homebrew" voting card. Further, because the actual voting booths a enclosed structures the researchers may be used to, it was inaccurately it would be easy to use a readily available device to capture the data wi The data which would be needed to create voting cards varies from elec so creating voting cards would be difficult without access to such captur

Unrealistic to tamper with results

Similarly, the suggestion that election results would be intercepted and uploading is unrealistic. First, any results transmitted via modem are al unofficial results. The official results are transported solely by means of which is locked into the system during voting, and manually transported central for results uploading following the voting process. Any modified would not match the official results and would immediately be rejected. very unlikely that any individual would have all the information required such an attack.

Change control process and testing validate software

Beyond the code analysis, the researchers suggested that Diebold Elec lacked an adequate change control process. Systemic control is in plac and externally. Diebold Election Systems' extensive change control pr embedded in its source code, nor would it be expected to be. In additio programming group and quality control, the software is tested externally testing authorities. Once delivered to the customer, the software is test accuracy both before and after each election An individual intent on in malevolent code, would require the cooperation of the programmers, th assurance group, the independent testing authorities, the multiparty ob workers.

Safeguards built into ballot creation

In addition, programmers draft code to deal with party IDs, candidate ID and other generic object identifiers, not individually identified candidate actual information associated with these identifiers is entered by individ particular election jurisdiction. Because the specific association betwee identifier and a particular candidate is not predictable in advance, it wo impossible for a programmer to craft programming to favor a particular political party without the active cooperation of the individual in the elec who formats the ballots. It is extremely unlikely that this kind of cooper in the first place or, if it did occur, would go unnoticed by the quality ass the independent testing authority, the multiparty observers, and poll wo

researchers. For example, without access to drives or a keyboard, an attack by changing registry entries or files would not be easily accomplished.

Layers of security prevent creating voting cards

Similarly, unlike the personal computer on which the analysis was performed, the card reader is an integrated portion of the voting terminal. This configuration renders realistically impossible the wire tapping necessary to capture the data required to create a "homebrew" voting card. Further, because the actual voting booths are not the enclosed structures the researchers may be used to, it was inaccurately suggested that it would be easy to use a readily available device to capture the data without detection. The data which would be needed to create voting cards varies from election to election, so creating voting cards would be difficult without access to such captured data.

Unrealistic to tamper with results

Similarly, the suggestion that election results would be intercepted and modified during uploading is unrealistic. First, any results transmitted via modem are always considered unofficial results. The official results are transported solely by means of a memory card, which is locked into the system during voting, and manually transported to election central for results uploading following the voting process. Any modified unofficial results would not match the official results and would immediately be rejected. In addition, it is very unlikely that any individual would have all the information required to implement such an attack.

Change control process and testing validate software

Beyond the code analysis, the researchers suggested that Diebold Election Systems lacked an adequate change control process. Systemic control is in place, both internally and externally. Diebold Election Systems' extensive change control process is not embedded in its source code, nor would it be expected to be. In addition to the internal programming group and quality control, the software is tested externally by independent testing authorities. Once delivered to the customer, the software is tested for logic and accuracy both before and after each election An individual intent on inserting malevolent code, would require the cooperation of the programmers, the quality assurance group, the independent testing authorities, the multiparty observers, and poll workers.

Safeguards built into ballot creation

In addition, programmers draft code to deal with party IDs, candidate IDs, precinct IDs, and other generic object identifiers, not individually identified candidates or parties. The actual information associated with these identifiers is entered by individuals in a particular election jurisdiction. Because the specific association between a generic identifier and a particular candidate is not predictable in advance, it would be nearly impossible for a programmer to craft programming to favor a particular candidate or political party without the active cooperation of the individual in the election jurisdiction who formats the ballots. It is extremely unlikely that this kind of cooperation would occur in the first place or, if it did occur, would go unnoticed by the quality assurance group, the independent testing authority, the multiparty observers, and poll workers.

Each vote is secure

The democratic process is a fiercely held right in this country, and election officials have long been on guard against mishap and fraud. They have implemented a comprehensive list of safeguards, which protect the integrity of the election process. These safeguards did not end when electronic voting entered the picture, and in fact have been increased. Electronic voting offers an opportunity to make voting more accessible and independent than ever before, particularly to individuals who are sight impaired or who speak another language. To require that each portion of the system be impervious to security breaches ignores security features in place in each other element of the physical system, and the systemic protections in place that extend far beyond the devices on which the votes are cast and tallied.

Diebold Election Systems is a wholly owned operating subsidiary of Diebold, Incorporated, a global leader in providing integrated self-service delivery systems and services. Diebold employs more than 13,000 associates with representation in more than 88 countries worldwide, and is headquartered in North Canton, Ohio, USA. Diebold reported revenue of $1.9 billion in 2002 and is publicly traded on the New York Stock Exchange under the symbol 'DBD.' For more information on Diebold Election Systems, Inc., visit the company's Web site at www.dieboldes.com, or call 1-800-433-VOTE.

DIEBOLD
ELECTION SYSTEMS

July 30, 2003

Checks and balances in elections equipment and pr prevent alleged fraud scenarios

Diebold Election Systems has concluded that the recent voting systems conducted by Associate Professor Aviel Rubin alleges scenarios that cc within an actual election process due to the checks and balances within equipment and those found in accepted election procedures.

On July 23, 2003, a team of students, directed by Rubin and Assistant F Wallach, issued a report to the media alleging serious security flaws in Systems' AccuVote®-TS.

Following this executive summary is a detailed rebuttal of the flaws and the Rubin report. The problems with the report fall into four major categ

- Lack of presentation and/or understanding of the full electoral pr
- False technical assumptions
- Inadequate research methodology
- Insufficient input from election experts

The Diebold AccuVote-TS touch screen voting station is just one eleme process that is highly regimented and that has evolved and been honed of years in the United States. When developing their various election fra the authors of the report focused solely on the part the AccuVote-TS so the voting process, while ignoring the other critical checks and balances electoral system. The authors' expressed assumptions include fundame misunderstandings of the overall election process - whether making use electronic voting systems or traditional papers ballots.

An election is a very public event. Every critical process throughout an e verified by third parties to ensure the integrity of the electoral system. These checks and balances include:

- Equipment Certification – Voting equipment is certified by the Natior State Election Directors and generally by the state certification expe
- Equipment Purchase – Through an independent committee or an ap board, a county, state or municipality evaluates and chooses electio
- Equipment Receipt - Contracts authorized by local election boards F of election equipment generally include mandatory acceptance testi that all the voting equipment meets their standards.

DIEBOLD®
ELECTION SYSTEMS

July 30, 2003

Checks and balances in elections equipment and procedures prevent alleged fraud scenarios

Diebold Election Systems has concluded that the recent voting systems report conducted by Associate Professor Aviel Rubin alleges scenarios that could not occur within an actual election process due to the checks and balances within the actual equipment and those found in accepted election procedures.

On July 23, 2003, a team of students, directed by Rubin and Assistant Professor Dan Wallach, issued a report to the media alleging serious security flaws in Diebold Election Systems' AccuVote®-TS.

Following this executive summary is a detailed rebuttal of the flaws and inaccuracies of the Rubin report. The problems with the report fall into four major categories:

- Lack of presentation and/or understanding of the full electoral process
- False technical assumptions
- Inadequate research methodology
- Insufficient input from election experts

The Diebold AccuVote-TS touch screen voting station is just one element of the electoral process that is highly regimented and that has evolved and been honed over hundreds of years in the United States. When developing their various election fraud scenarios, the authors of the report focused solely on the part the AccuVote-TS software plays in the voting process, while ignoring the other critical checks and balances present in our electoral system. The authors' expressed assumptions include fundamental misunderstandings of the overall election process - whether making use of modern electronic voting systems or traditional papers ballots.

An election is a very public event. Every critical process throughout an election cycle is verified by third parties to ensure the integrity of the electoral system.
These checks and balances include:

- Equipment Certification – Voting equipment is certified by the National Association of State Election Directors and generally by the state certification expert, as well.

- Equipment Purchase – Through an independent committee or an appointed elected board, a county, state or municipality evaluates and chooses election equipment.

- Equipment Receipt - Contracts authorized by local election boards for the purchase of election equipment generally include mandatory acceptance testing, to confirm that all the voting equipment meets their standards.

Statement of Jim Knox
Executive Director, California Common Cause
July 1, 2003

Disability rights, civil rights and good government groups today call State Kevin Shelley to act to ensure that the voting rights of millions are enhanced and protected—not infringed upon.

We are at an historic crossroad in the history of voting in California. has mandated that California's antiquated and inaccurate punch ca machines be replaced in time for the March 2004 election. Passag act, Proposition 41, and the federal Help America Vote Act will prov the direction to purchase state of the art, easy to use touchscreen v

These machines are already in use in parts of California and have accurate type of voting machine, and the easiest to us. Touchscre machines will make it possible for millions of California voters with easily and independently for the first time. Touchscreen voting ma voters from inadvertently voting for more than one candidate per ra their ballot subsequently disqualified. Touchcreen voting machines shown to greatly reduce the disparity which now exists between dis cast by whites and discarded ballot cast by minorities. Touchscreen make it much easier for limited English speaking voters to vote bec can be changed to more than a dozen languages at the touch of a for limited literacy voters to vote because the information is availabl headphones.

But the transition to these far preferable machines is now being blo arguments that touchscreen voting machines should be required to paper replicas to each voter at the time each voter votes. While thi initially has superficial appeal, further study indicates that this featu & unproven. Failure to resolve this issue has driven a number of th must convert to new machines to abandon their plans to move to to instead choose optical scan machines

In February, the Secretary of State convened a task force to resolve work of this commission was completed six weeks ago, but has yet We call upon the Secretary of State to release this report and remo confusion that has been allowed to hang over this issue. Until this i counties faced with having to buy new voting machines have reaso state may require this unnecessary and as yet unproven feature. A counties have abandoned their plans to purchase touchscreen mac

Statement of Jim Knox
Executive Director, California Common Cause
July 1, 2003

Disability rights, civil rights and good government groups today call upon Secretary of State Kevin Shelley to act to ensure that the voting rights of millions of Californians are enhanced and protected—not infringed upon.

We are at an historic crossroad in the history of voting in California. A court order has mandated that California's antiquated and inaccurate punch card voting machines be replaced in time for the March 2004 election. Passage of a state bond act, Proposition 41, and the federal Help America Vote Act will provide the funds and the direction to purchase state of the art, easy to use touchscreen voting machines.

These machines are already in use in parts of California and have proven to be most accurate type of voting machine, and the easiest to us. Touchscreen voting machines will make it possible for millions of California voters with disabilities to vote easily and independently for the first time. Touchscreen voting machines will prevent voters from inadvertently voting for more than one candidate per race and having their ballot subsequently disqualified. Touchcreen voting machines have been shown to greatly reduce the disparity which now exists between discarded ballots cast by whites and discarded ballot cast by minorities. Touchscreen voting machines make it much easier for limited English speaking voters to vote because the screen can be changed to more than a dozen languages at the touch of a button, and easier for limited literacy voters to vote because the information is available audially through headphones.

But the transition to these far preferable machines is now being blocked by arguments that touchscreen voting machines should be required to provide duplicate paper replicas to each voter at the time each voter votes. While this argument initially has superficial appeal, further study indicates that this feature is unnecessary & unproven. Failure to resolve this issue has driven a number of the counties which must convert to new machines to abandon their plans to move to touchsreens, and instead choose optical scan machines

In February, the Secretary of State convened a task force to resolve this issue. The work of this commission was completed six weeks ago, but has yet to be released. We call upon the Secretary of State to release this report and remove the cloud of confusion that has been allowed to hang over this issue. Until this issue is resolved, counties faced with having to buy new voting machines have reason to fear that the state may require this unnecessary and as yet unproven feature. As a result, some counties have abandoned their plans to purchase touchscreen machines and instead

have been forced to choose less preferable optical scan machines. Optical scan machines offer none of the easy to use features of touchscreen machines and in particular disadvantage persons with disabilities, linguistic minorities and people of color.

In order to seize upon this once in generation opportunity to greatly enhance and protect the voting rights of millions of Californians, we call upon the Secretary of State to release the task force report, and to oppose the ill-conceived calls to mandate duplicate paper replicas.

THE LEAGUE OF WOMEN VOTERS®
OF THE UNITED STATES

Questions and Answers on Direct Recording Electronic (DRE) Voting Systems

QUESTION: What is the controversy over Direct Recording Electronic (DRE) voting systems?

ANSWER: Some claim that electronic voting machines are subject to manipulation that will allow votes to be stolen, and that the only way to protect against this is to have a voter verified paper trail (VVPT). The concerns come in three areas. First, some say that a "Trojan Horse" computer chip or special code could be installed in the voting machine by the manufacturer or another "insider" that would cause votes to be incorrectly recorded. Second, some suggest that the machine could be penetrated ("hacked") or that the management security systems could be bypassed to allow an outsider to manipulate the voting machine. Finally, some observers are concerned that linking voting machines electronically or using the Internet to transmit election results will allow results to be manipulated.

QUESTION: Is this something that I should worry about, as a voter?

ANSWER: There is no reason to believe that a well-run election system based on DREs will steal your vote. In fact, modern voting systems like DREs and precinct-count optical scan voting systems can be much better than the punchcard voting machines and lever machines that they are replacing. At the same time, it is important that election officials put management safeguards in place to ensure that all voting systems function properly.

QUESTION: Then why is there such a debate?

ANSWER: The concern about electronic voting machines taps into deep reservoirs of distrust: distrust of the election systems that were so flawed in 2000, distrust of new technologies; and basic distrust of the political system. Many Americans became deeply concerned after the 2000 election revealed the problems that plague our election systems. "Hanging chads" were just part of the problem as Americans learned about such issues as voting machines that don't work well, poor ballot design, and people being turned away from the polls because of poor administration of voter rolls, including erroneous purging. In addition, many people are uncomfortable with or distrustful of new technologies, even though we rely on such technologies to fly our airplanes and operate our banking systems so long as there are appropriate management systems to provide safeguards. Finally, computer specialists with limited experience with election systems have focused narrowly on the DRE machines themselves without taking into account the management systems and safeguards that can protect against tampering and without acknowledging the problems associated with other voting systems such as punchcard machines.

1730 M STREET, NW, SUITE 1000, WASHINGTON, DC 20036-4508
202-429-1965 FAX 202-429-0854
Internet: http://www.lwv.org E-mail: lwv@lwv.org

QUESTION: What are DREs?

ANSWER: Direct Recording Electronic (DRE) voting systems are one of two types of modern voting machines; the other is the precinct-count optical scan system. Both these systems are improvements over older systems such as punchcard machines, lever machines, paper ballots, central-count optical scan machines and a previous generation of older computer machines. The DRE is also called a "touchscreen" voting machine or an electronic voting machine. The voter touches a computer screen to vote for each candidate or issue, has an opportunity to review the ballot, and then casts the ballot on the electronic machine.

QUESTION: What are the advantages of DRE systems?

ANSWER: There are a number of advantages to DRE systems. They can easily be adapted with earphones and other devices so that persons with disabilities can cast ballots independently and in private, and they are easily adapted for multiple languages. They directly record votes so they provide accurate counts, and there must be a paper record of all the votes cast on each voting system. DREs provide for "second chance" voting in private, so that a person who makes a mistake in voting can automatically be notified and make a correction to the ballot before it is cast. In the case of an "overvote," where a person mistakenly votes for more than one candidate for an office such a President, the machine can automatically prevent the error in the first place. Studies indicate a high degree of acceptance of DREs by voters, of all ages and ethnic and racial backgrounds, who have used them. DREs also reduce many of the operational problems in handling paper ballots that have sometimes led to election irregularities. As discussed in this document, there is controversy over the security of DRE machines.

QUESTION: What are precinct-count optical scan voting machines?

ANSWER: Optical scan machines use a ballot printed on special paper that is then marked by the voter, usually with a #2 pencil or with a special marker. The ballot is then fed into a counting machine that reflects light off the markings to scan and count the vote. Central-count optical scan systems, where the ballots are collected and sent to a central location before being scanned, cannot provide for "second chance" voting, as is required by the Help America Vote Act (HAVA), because the voter cannot make a correction to the ballot. With precinct-count optical scan systems, the voter or an election official puts the ballot in the scanner at the polling place. If there is a problem, such as an "overvote," the scanner returns the ballot for correction by the voter. Central count is used for mail-in and absentee voting.

QUESTION: What are the advantages of precinct-count optical scan systems?

ANSWER: There are a number of advantages and disadvantages for precinct-count optical scan machines. The initial costs of such systems are lower than for DREs, but the costs of printing the ballots on the special paper raise the costs over the long run. Because they are based on marking a paper ballot, persons with physical disabilities and those who are blind or have declining vision, such as the elderly, have trouble with these systems. In addition, the process for "second

chance" voting is not private: if the scanner sees a problem, the election official returns the ballot to the voter, a potentially embarrassing and perhaps intimidating process. Localities with significant numbers of voters who would benefit from a ballot in a language other than English, but which are not required by federal law to offer such ballots in those languages because the number of such voters is not sufficiently large, will not offer ballots in multiple languages because of the costs of printing the ballots. The optical scan ballots can be recounted, but there have been reliability and repeatability concerns in some elections.

QUESTION: What are some of the safeguards that can protect against a malfunctioning voting machine?

ANSWER: Voting machines are scrutinized by state officials and computer specialists before a machine is certified for use in their states. Voting machines are also tested to guard against malfunctions, and management systems guard against error and ensure that unauthorized personnel do not have access to the machines. Testing and monitoring typically occurs many times in well-run systems: First, voting machines must meet nationally certified design standards in most states. Second, the individual machines are tested when they are delivered by the manufacturer to election officials. Third, the machines are tested just before Election Day. Fourth, and especially important, the machines are monitored during Election Day. Finally, the machines are tested after Election Day. Security measures prevent tampering after each stage of the process. Each of these tests helps guard against the use of a malfunctioning machine, and, taken together, suggests a high degree of reliability. Of course, as with any system, if the safeguards are not followed, then problems can result.

QUESTION: But I have heard that you can't test a machine in operation, only in "test mode." What protects against a "Trojan Horse" computer chip or code that a manufacturer or other insider might put in a machine? Couldn't it be programmed only to manipulate the vote on Election Day, and not be active at any other time?

ANSWER: Voting machines can be tested in "election" mode. Not only can the tests be designed to simulate the specific conditions under which the machines will be used on Election Day, the internal clock on the machine can be adjusted to assure that the machine "thinks" it is running in real time on Election Day, when it is, in fact, being tested. Some have suggested that the "Trojan Horse" could contain its own clock or other mechanism that would activate only on the real Election Day and that it could bypass the testing. However, computer specialists point to testing and monitoring on Election Day as an additional safeguard against this scenario. The best tests include randomly taking a machine out of service to run "test votes" to verify accuracy. This should be done with people from all interests represented. Since current voting machines do not use special technology to guard against external break-ins, one key safeguard is to ensure that voting machines are not linked together, or linked on the Internet, because such connections could allow rogue programs to penetrate the system after testing.

QUESTION: What are the safeguards that protect against outside interference? Couldn't a technologically adept voter vote several times?

ANSWER: There are a variety of management safeguards to protect against outside interference. The most important ways are to ensure that voting machines are not linked together or linked on the Internet, and that results are not transferred directly from the machines over phone lines. Isolating each machine ensures that any possible problem with one machine does not contaminate the system as a whole, making it much more difficult to affect an election. Isolating machines from the Internet and from phone lines prevents entry into a voting system through those routes. Other safeguards include restricting physical access to machines and setting up polling place operations that monitor machine usage, including the number of votes being cast. To tamper with a DRE someone would need to know each of the security systems within the machine, including codes, formats and storage capacities, and be able to manipulate them undetected after first gaining sufficient access to spend the necessary time with the machine. DREs are not an election system unto themselves; they are simply an instrument within a complex election system. It is the interaction of the technical, physical, and procedural security measures that actually secure the voting system, not any one of these measures alone. The key is to have an overall system that builds in multiple checks making it improbable that the system will be tampered with.

QUESTION: I heard that the new Maryland voting system was challenged because of security concerns.

ANSWER: The governor of Maryland ordered a review of Maryland's new DRE voting systems after a report from a professor at Johns Hopkins University suggested that security could be breached. The independent security analysis done for the state by Science Applications International Corporation (SAIC), an independent IT firm with an international reputation in IT security, found that DREs can work effectively, but, like all systems, need good management systems to ensure the reliability and integrity of the voting process. A number of recommendations were made, including isolating the system from any network connections, appointing a chief security officer, developing a formal set of policies and procedures through all jurisdictions, and creating a formal security plan using recognized "best practices." None of the recommendations by SAIC included the use of a voter verified paper trail (VVPT).

QUESTION: I heard that the voting machine computer codes are kept secret and that computer professionals are prohibited from working with the machines by copyright laws and other regulations. How can we be sure that voting machines work properly if outside testers cannot get into the systems? Don't we need "open codes" and to allow "reverse engineering" in order to test the security of voting machines?

ANSWER: Computer experts, retained by election officials under confidentiality agreements, currently review and evaluate computer codes and systems in the testing and evaluation of voting systems. In addition, secrecy is an important security measure. Limiting access to computer codes in DREs is important in protecting the voting system. If those who might want to

penetrate the system already know all the details of that system, it is much easier to breach security. "Open codes" can compromise security. However, it is vital that election officials have access to all design and other information about voting systems so that the machines can be certified, tested, and programmed with appropriate ballots. It is also important that responsible government officials and appropriate independent test authorities have reviewed the code and have control over the system, rather than relying on outside manufacturers or suppliers. As in any system, the expertise of managers and computer specialists is crucial in monitoring the practices of manufacturers and suppliers.

QUESTION: Are election results transmitted over the Internet? Doesn't that allow the totals to be changed by a "hacker?"

ANSWER: Most agree that connecting voting systems on-line substantially increases the risk that they can be penetrated. That's why well-managed systems are not kept on-line. Sometimes unofficial election results are transmitted over the Internet, but this should not be done directly from the voting machines. Security can be improved when transmittals are made at random times and are encrypted. More importantly, in well-run systems official results are computed directly from the memory cards and are not certified until they are double and triple checked with results that are not transmitted electronically.

QUESTION: What is a voter verified paper trail or VVPT?

ANSWER: A VVPT is an add-on system that prints out the voter's individual ballot choices after they have been cast on the DRE. Proponents of the voter verified paper trail argue that this allows the voter to confirm his or her votes and that it provides an opportunity for recounts since the paper record of each individual ballot is retained by election officials. The term is used interchangeably to refer to systems that simply provide the individual paper record and systems that would require that each voter actually verify the paper record of his or her vote.

QUESTION: Why don't we require a voter verified paper trail as part of DRE voting machines? Won't having a paper record of every individual vote protect the integrity of the election system?

ANSWER: There are a number of problems with requiring a voter verified paper trail as part of DREs. The most significant is that the VVPT does not provide a safeguard against the supposed problem: a machine that is programmed to record the incorrect vote. If the machine can be programmed to record the wrong vote, then it can be programmed to print out a misleading confirmation. Advocates say that the individual ballot paper confirmation can be recounted, to guard against this problem. However, a very important problem remains: The VVPT paper ballots are difficult, if not impossible, to recount consistently, leading to inaccuracies. The paper printed out from many of the add-on printers for DREs use script paper, like that in an ATM, or thermofax paper, like that in fax machine. It is not possible to recount that paper except by hand, a process that is extraordinarily cumbersome and inaccurate. Even if better paper were used, all the problems inherent in a paper ballot recount would be in place. These include questions about

mutilated or hard-to-read ballots, the possible loss or manipulation of the paper ballots, and the fact that no two recounts yield the same result. In short, the voter verified paper trail does not provide a real safeguard and it has significant operational problems. The best safeguards are those discussed above – certification, testing and management systems for DREs, as well as all other voting systems.

QUESTION: Is the DRE a paperless system? Aren't there any records?

ANSWER: Under the Help America Vote Act (HAVA) there must be a paper record of each vote from a DRE voting system. In well-run systems, the printouts with vote totals are taken throughout Election Day and compared to the total number of votes cast at the machine, to ensure security. The paper records then provide a backup for official tabulations of election results. In addition to vote totals, DREs can print out each individual ballot (without identifying the voter) to provide an additional security and audit capacity. Not only can this data be printed, it is saved electronically in multiple formats in multiple locations, so that if one mechanism fails the information is backed up using another format in another location. In other words, DREs in well-administered systems provide a substantial audit capacity for purposes of recounts and authentication.

QUESTION: What are some of the other issues with a requirement for a voter verified paper trail?

ANSWER: One important advantage of a DRE system is that it provides an opportunity for persons with disabilities and people with limited English capacity to vote privately and independently. The DRE is easily fitted with earphones for an aural ballot for persons with limited vision, including the elderly, and for persons with limited reading ability. For persons with physical disabilities, the computer interface system is easier to use than the optical scan system which requires the voter to successfully manipulate the marking pencil. For persons with limited English capacity, DREs can easily be programmed to accommodate multiple languages. A requirement for the voter to verify a paper ballot undermines access for citizens who have trouble seeing or who have limited English capacity, and can push election officials toward optical scan devices that are not as accessible for a broader range of citizens.

QUESTION: Are there operational questions about the voter verified paper trail?

ANSWER: Yes. Printers are among the least reliable of computer system components. They jam, they need paper, they are slow, and they are an added cost. Long lines are already a problem in many voting jurisdictions, and printing individual ballots for confirmation by each voter at the polling place will only exacerbate those problems, without adding to security. Voters' privacy is also at risk each time a printer jams and a poll worker has to work to remove the paper jam. Finally, the verification process in this format can be confusing to the voter and has not been fully tested in polling place operations.

QUESTION: Are there security and accuracy issues with the voter verified paper trail?

ANSWER: Yes, there are significant security issues with a system that requires each voter to review, in private, an individual piece of paper. Each individual piece of paper in the voter verified paper trail system must be collected, protected, and prepared for a recount. As we saw in Florida in 2000, with nearly 6 million ballots cast in the Presidential election, this is a monumental task, with the possibility of lost, mangled and manipulated paper ballots. With these well-known problems with paper recounts, it is more likely that the paper recount would be in error than the electronically cast ballots from DREs with their required paper back-up records. In fact, when asked what would happen if there were a question about the accuracy of results with a voter verified paper trail system, one manufacturer of such devices, and an advocate for the VVPT, said that of course they would do a recount using the electronic systems. They would not even try to recount the individual paper confirmations.

QUESTION: Is there an issue with certification of machines that can provide a voter verified paper trail?

ANSWER: Approximately 40 states have chosen to follow the federal voluntary standards for certifying their voting systems. These standards are designed to ensure that voting machines meet basic reliability and security requirements. These standards and procedures do not currently provide for a voter verified paper trail. Developing standards takes a period of time to make sure that issues are properly addressed. The issues for the VVPT include what kinds of paper would be used, how it would interface with DRE machines, how the voter would verify or refuse to verify the paper record, how the individual paper confirmations would be handled and protected, and a host of other technical issues. Even if a VVPT requirement were advisable, there are serious practical and legal problems that must be resolved before moving ahead.

QUESTION: Is there any protection to ensure my ballot says what I intend it to say?

ANSWER: The new Help American Vote Act (HAVA) already requires that voting systems provide for "second chance" voting by 2006. While many had hoped for an earlier deadline, the practicalities of changing many voting systems quickly caused Congress to choose the 2006 deadline. Nonetheless, new machines being purchased now must meet the "second chance" voting requirement. That requirement means that before your ballot will be officially cast, you must have the opportunity to review it, change it, or request a new ballot. The voting system must also notify you of a possible "overvote" (such as voting for two candidates for President) so that you can make a correction. For DREs, this process occurs in the privacy of the polling place, the machine itself is programmed to make it difficult to make a mistake, and the system gives the opportunity to review the ballot before it is cast. With optical scan and punchcard ballots, the review function comes as the paper ballot is sent through a machine with the poll worker and other voters looking on. Finally, under HAVA, as described above, there must be a paper record of each vote from each voting system.

QUESTION: Haven't we always relied on paper. What about recounts?

ANSWER: Much of the country has voted on lever machines for the past century. With lever machines, a recount consists merely of reading the machine again, without the benefit of an individual record of each vote cast, as DRE systems can provide. Human errors in reading the machines and counters that stick are real problems for lever machines. Paper ballots get recounted because of the inherent inaccuracies associated with the counting of paper ballots. When thousands of pieces of paper are counted, either by hand or by machine, mistakes are made, and so recounts are often needed if the margin of victory is small. Punchcards were a major advance over regular paper ballots because they are counted by machine. The problem, as we saw in Florida in 2000, is that the marking system (punching through the paper so the machine can count it) is sometimes incomplete (the "hanging" or "dimpled" chad). Similarly, optical scan systems sometimes have a marking problem, because the pencil used is not the correct one and so does not reflect the vote when the machine scans the paper ballot, or because the voter "incorrectly" marks the ballot with an X or incompletely marks the ballot. So recounts are necessary with paper ballots because of the inherent problems with paper ballots. Electronic machines do not have this problem. The accuracy of the counting is not really at issue. The issue with electronic systems, as discussed here, is whether the machine is accurately receiving the information from the voter. To guard against possible errors after the ballots are cast, new standards under HAVA require a paper record of each vote, as discussed above. From the recount angle, DREs are clearly better than paper-based systems. Brazil regained trust in the election process by replacing a fraud-ridden paper system with DREs in the late 1990s.

QUESTION: I've heard that there is a question about election fraud in systems with paper receipts. What's that about?

ANSWER: If the voter is given a receipt that shows how he or she voted, then vote-buying schemes can be very effective and voter intimidation can ensue. Because of the paper record, the vote buyer knows that the seller voted according to the wishes of the purchaser. If voters have a record of how they voted, then spouses, employers and others can ask voters to disclose how they voted or "pay a penalty." For these reasons, no system should allow a voter to take a voter-verified ballot confirmation out of the polling place.

QUESTION: If a voter verified paper trail makes people feel good, why not do it?

ANSWER: The voter-verified paper trail adds costs and complications to the voting process, does not add significant security, and undermines disability and language access. To summarize: First, the voter verified paper trail is not necessary. Other mechanisms can provide necessary safeguards against security concerns. Second, the voter verified paper trail doesn't work. The individual paper records cannot be used accurately for a recount. Third, the voter verified paper trail requirement undermines access for persons with disabilities and limited English skills. Fourth, the voter verified paper trail doesn't add reliability to the system at the polling place. It complicates the polling process while the monitoring of machines during Election Day provides a similar safeguard. And fifth, the voter verified paper trail does not address the real election

system problems that caused nearly six percent of votes to be lost in 2000, including registration database failures, ballot design problems and polling place operations. In short, VVPT can mislead the public into believing that the paper confirmation is a valid record of the vote.

QUESTION: Our election system is so important. Shouldn't we insist that all voting systems have 100 percent accuracy?

ANSWER: Yes, we should aspire to have perfection in our voting systems and continually work toward that goal. Technological advances over the years have vastly improved our voting systems. It would be difficult to imagine counting the millions of votes that are cast in a Presidential election without those improvements over the old hand-counted paper ballot. In their day, punchcards and lever machines were substantial improvements. But they have significant problems, such as "hanging chads" and mechanical errors. Marking, transporting, storing and counting paper ballots have been the sources of election irregularities in some areas. And so we are moving to better systems like DREs and precinct-count optical scan machines. Improvements will continue to be made even in these systems, particularly in the area of the "human interface," to ensure they are "user friendly."

QUESTION: What is the role of the new federal Election Assistance Commission (EAC) set up under HAVA?

ANSWER: Once it is up and operating, the new federal EAC will have authority for the standard setting process for voting machines, in association with the National Institute of Standards and with the input of state election directors. The EAC will also develop best practices for election administration, examine emerging issues in election reform, and develop guidelines for the state certification process. The delay in nominating and confirming the four commissioners has delayed the EAC's work, which would include examination of potential security issues and deal with certification, testing and administrative practices to ensure voting machine security.

QUESTION: Why are voter education programs so important?

ANSWER: When voters have had experience using their voting machines, there are many fewer errors in properly recording the voters' intent. Even a machine that does not work particularly well can have a low error rate if the voter is familiar with the machine, while even a good voting system can have problems if voters are seeing it for the first time. Thus voter education programs, that explain how to work the voting machines and give voters an opportunity to practice and gain hands-on experience before Election Day, are very important.

QUESTION: What about Internet voting?

ANSWER: Voting over the Internet raises substantially more security issues because the voting machines and the official election site can be subject to penetration and manipulation. Many

hope that on-line voting will be a part of future elections, but there are many issues that must be resolved before we can have confidence in such systems.

QUESTION: I've heard that Miami replaced its voting machines after the 2000 election and still had problems in the 2002 election?

ANSWER: Miami-Dade County replaced its punchcard voting machines with new DREs for the 2002 election. Because of inadequate poll worker training, many of the machines were not plugged in, turned on or warmed up before the primary election, and there was confusion at the polls. For the general election, county and other officials were brought in to work at the polls, and the election proceeded more smoothly. This indicates, once again, how important it is that there be an integrated approach to improving voting systems. Good machines are needed, but so too is poll worker training and good administration.

QUESTION: What are the most important problems in our election systems?

ANSWER: The 2000 election exposed a large number of very serious problems in our election systems, from voting machines that don't work well to poor ballot designs, from erroneous purges to eligible voters being turned away from the polls because of poor administration of the voter rolls. According to an official report from the California Institute of Technology (Caltech) and the Massachusetts Institute of Technology (MIT), four to six million votes were lost in the 2000 Presidential election. Between 1.5 and two million were lost because of faulty voting equipment and confusing ballots, 1.5 to three million were lost because of voter registration mix ups, and up to one million were lost because of polling place operations. Congress responded by passing the Help America Vote Act (HAVA) which requires states to improve election administration and protect voting rights through new federal requirements, including provisional ballots, statewide computerized voter lists, "second chance" voting that helps to ensure the proper casting of ballots, and disability access. In addition, states were required to develop election reform implementation plans, which each of them has now done. Federal funding is being provided to implement the reforms described in state implementation plans.

QUESTION: What's the bottom line on DREs?

ANSWER: DREs, like all voting systems, must be carefully designed and tested, and there must be rigorous security and management systems. DREs bring important advantages to the election system, including ease of use, and disability and language access, while precinct-count optical scan machines can be an option as well for states upgrading their voting machines.

QUESTION: Where can I get more information?

ANSWER: The League of Women Voters website, at http://www.lwv.org/join/elections/hava_resources.html has additional background information, including papers by recognized experts in the field.

ELECTIONS & VOTING

THE LEAGUE OF WOMEN VOTERS®

Help America Vote Act

ACLU Statement of Principles on Touch Screen (DRE) Voting Systems

The integrity of the voting process is fundamental to the operation of our democracy. A major component of a valid electoral process is voting technology that honestly and accurately counts every ballot. Because voting technologies have always been susceptible to error, bias, and corruption, we must remain vigilant about new technologies and insist that they maximize the likelihood of recording what each voter intends, regardless of the voter's race, economic status, or geographical location. To this end, we must require that voting machines be accessible to all voters by reducing barriers to participation erected by language, physical disability, or complexity. Because democracy also requires that the public have confidence in the results of elections, we must ensure that voting technologies may not be rigged in a way that would thwart the true will of the electorate.

Though the now discredited punch-card voting systems failed all these tests, there is much debate about what voting systems should take their place. Touch screen voting systems offer tremendous potential advantages, including ease of use, accessibility to persons with disabilities, ready accommodation of the needs of language minorities, and the voter's ability to review and correct ballots. However, computer security experts have raised serious concerns about whether those machines are open to undetectable error, tampering, or outright fraud. Moreover, recent experience with the use of touch screen voting machines in California and Florida illustrate that these machines are vulnerable to more prosaic problems such as getting the machines up and running, inadequate training of poll workers and others responsible for overseeing the use of the machines, and instances in which manufacturers have not lived up to their representations concerning the machines, e.g. the support for multiple languages.

The ACLU strongly supports the recommendation of computer experts that digital voting technologies be subjected to the most rigorous testing and certification procedures. This should include rigorous and public testing of the software used in these systems.

The Voter-Verified Paper Ballot

105

Some computer experts have recommended the inclusion o contemporaneously created, "voter-verified" paper ballot tl become the ballot of record in the case of a disputed electic ACLU has serious reservations about the both the effective practicality of this proposal for the following reasons:

1. **Election officials would resort to a "verified pape in the case a recount or contest, which a hacker c or deter.** In most jurisdictions, recounts are triggered only wl is close. Thus, anyone savvy enough to hack into a digital syste election results would simply select a margin of victory big enc a recount or discourage a contest. In these jurisdictions, a comp could block the review of any paper ballots. Even in those few like California, which automatically conduct a recount of a sma of the ballots, a sophisticated fraud could thwart detection by c code for the paper printout. (See paragraph 2 below)
2. **The voter-verified paper trail could be used by a sophisticated fraud to give voters a false sense of s their vote was correctly tallied.** For example, if the con genuinely vulnerable to attack, a competent hacker could not o it to make the machine record a fraudulent vote, but could also the code that runs the printer, causing it to display the voter's ir machine records the fraud.
3. **There is no reason to assume that paper recounts accurate than DRE machine tabulations.** Paper is nc difficult to handle and easy to manipulate. Counting the paper t generated by DREs would be subject to all of the historical pro associated with paper ballots, including human error, fraud, anc
4. **The reliability of printers has never been systema tested in conditions similar to those that exist in p places on Election Day**.

Recommendations

The ACLU believes that the voter verified paper ballots sh be employed until there has been a rigorous test of their rel practicality in circumstances comparable to their use on El This review should include a consideration of the possibilit error and fraud in handling these ballots.

In the interim, if DRE's are to be employed in the 20 election cycle:

1. **The computer source code for all security c functions of the machines should be subject thorough independent review.** "Open Source C which can be freely tested, is the best solution to the prc of computer software integrity. At a minimum, the full t should be subjected to a review by an independent body only open source code should be used for tabulating the
2. **Rigorous physical security measures need tc instituted** to insure that the machines and any associa paper ballots are not compromised.

Some computer experts have recommended the inclusion of a contemporaneously created, "voter-verified" paper ballot that would become the ballot of record in the case of a disputed election. The ACLU has serious reservations about the both the effectiveness and practicality of this proposal for the following reasons:

1. **Election officials would resort to a "verified paper trail" only in the case a recount or contest, which a hacker can prevent or deter.** In most jurisdictions, recounts are triggered only when an election is close. Thus, anyone savvy enough to hack into a digital system and alter election results would simply select a margin of victory big enough to prevent a recount or discourage a contest. In these jurisdictions, a competent hacker could block the review of any paper ballots. Even in those few jurisdictions, like California, which automatically conduct a recount of a small percentage of the ballots, a sophisticated fraud could thwart detection by corrupting the code for the paper printout. (See paragraph 2 below)
2. **The voter-verified paper trail could be used by a sophisticated fraud to give voters a false sense of security that their vote was correctly tallied.** For example, if the computer code is genuinely vulnerable to attack, a competent hacker could not only compromise it to make the machine record a fraudulent vote, but could also compromise the code that runs the printer, causing it to display the voter's intent while the machine records the fraud.
3. **There is no reason to assume that paper recounts are more accurate than DRE machine tabulations.** Paper is notoriously difficult to handle and easy to manipulate. Counting the paper ballots generated by DREs would be subject to all of the historical problems associated with paper ballots, including human error, fraud, and mishandling.
4. **The reliability of printers has never been systematically tested in conditions similar to those that exist in polling places on Election Day**.

Recommendations

The ACLU believes that the voter verified paper ballots should be not be employed until there has been a rigorous test of their reliability and practicality in circumstances comparable to their use on Election Day. This review should include a consideration of the possibility for human error and fraud in handling these ballots.

In the interim, if DRE's are to be employed in the 2004 election cycle:

1. **The computer source code for all security critical functions of the machines should be subjected to thorough independent review.** "Open Source Code", which can be freely tested, is the best solution to the problem of computer software integrity. At a minimum, the full the code should be subjected to a review by an independent body and only open source code should be used for tabulating the results.
2. **Rigorous physical security measures need to be instituted** to insure that the machines and any associated paper ballots are not compromised.

107

3. **Election officials need to be thoroughly trained in their use and the physical infrastructure necessary to insure their use, e.g. sufficient electrical wiring, needs to be assured.**
4. **The jurisdiction should have a permanent broad-based security task force or oversight body,** representing all interested segments of the community, to evaluate the potential for fraud or error in voting systems and to address the new security challenges that will inevitably arise in the future. That task force should have complete access to the DRE code and conduct its own independent testing.
5. **Election officials should select technology that gives them maximum flexibility in taking advantage of emerging technological innovations,** including the incorporation of printer that will provide a voter-verified paper ballot for use with touch screen systems, if such technological innovations are shown to be feasible and to enhance the integrity of the voting process.

If an election jurisdiction chooses to employ optical scan or a method other than DREs for its general balloting, it should:

1. **Be required to have a sufficient number of DREs available to accommodate the needs of persons with disabilities and,**
2. **Employ systems that can accommodate the needs of language minorities.**

Finally, the ACLU believes that the debate over the voter verified paper ballot has obscured other important issues that bear greater scrutiny. We believe there needs to be:

1. **An evaluation of the new generation of touch screen machines only now being developed** and, in some cases, used in nations such as Brazil and Australia, and those being developed in the US by non-partisan and non-profit institutions. The review should especially focus on those systems, e.g., the Australian system, which are based on open source code.
2. **Thorough and independent studies of the error rates including "lost ballots" that fail to record, as well as over and under votes, of the two newer voting technologies** most likely to be employed in 2004 election-- touch screen and optical scan ballots.
3. **An analysis of existing testing and certification procedures for all digitally-based voting technologies,** including both touch screen and optical scan voting technologies, to determine whether current procedures assure the integrity and security of all hardware, software, and any associated paper ballots.

Leadership Conference on Civil Rights

1629 K Street, NW
10th Floor
Washington, D.C. 20006

Phone: 202-466-3311
Fax: 202-466-3435
www.civilrights.org

ELECTION REFORM POLICY ANALYSIS:

"Voter-Verified Paper Trails" Are Not Needed To Keep Elections From Being Stolen

As outdated & infamous punch-card and lever style voting systems are steadily being phased out throughout the country, *direct recording electronic* ("DRE") or "ATM-style" voting machines are becoming more popular. Some people, however, have attacked these newer machines, claiming that they are dangerously prone to manipulation, and that hardware or software failures are especially susceptible to resulting in lost votes. Some have even gone as far as to suggest that new machines are being used as part of a conspiracy to rig elections around the country.

Many of these critics believe that their concerns would be best addressed if DREs produced a printed ballot, which, in theory, voters would examine to determine that their votes had been cast and counted properly. To this end, Rep. Rush Holt (D-NJ) has introduced the "Voter Confidence and Increased Accessibility Act" (H.R. 2239), which would go beyond current law – which was recently changed by the "Help America Vote Act" (HAVA) to require all voting machines to produce a printed audit trail – to add a new requirement that a "hard copy" of each ballot be verified by the voter before it is cast.

The integrity and reliability of the voting process is of the utmost importance, and the creation of electronic records that can be used for audits and recounts is essential. Technology that allows voters to check their ballots before casting them, as is required by HAVA, is also very important. However, many of the concerns that have been raised over the reliability and security of DREs are overstated or unwarranted. Furthermore, while calls for the production of a *voter-verified individual-ballot paper trail* by DREs may be well-intended, such a step would lead to a wide range of negative consequences.

Fact: DRE Systems Are Replacing Outdated, Failed Technologies

Current DRE systems are very popular replacements for outdated technologies like levers and punch cards. Those older systems often have high rates of error, are harder to use, are often inaccessible to people with disabilities, and are harder to adapt for people who speak different languages. Empirical evidence from use in the field suggest that touch screens are easier to use, including by the elderly & minorities, are more accurate, more accessible to voters with disabilities, and easier to adapt to different languages than older technologies.[1] DREs also *already* allow voters to verify their ballots before they are cast, by displaying a final ballot on screen to be confirmed. In many ways, DREs are a significant advance from a voter's perspective.

Fact: Security and Reliability Concerns With DRE Machines Have Been Exaggerated

DREs are highly sophisticated, with most of them storing ballot records in multiple formats and in multiple locations. Furthermore, DREs are already required under federal law to create records that can be audited, and most machines currently provide not only the total vote tallies but also a record of how each individual ballot was cast. In many cases, like the machines used in Georgia, DREs produce 3 records of the vote: the official count, a backup count on a separate chip, and a paper record printed out once polls close. In order to rig a DRE, an individual would need to be intimately familiar with its

[1] *See, e.g.* Michael Tomz & Robert T. Van Houweling, *"How Does Voting Equipment Affect the Racial Gap in Voided Ballots?,"* http://www.stanford.edu/~tomz/pubs/gap.pdf

software, gain access to it long enough to change its code, conceal the changes during pre- and post-election testing, and do this on enough machines to actually alter the outcome of an election. While such rigging is possible *in theory*, in practice it is highly improbable – in fact, in practice, it would be far easier to simply "lose" paper ballots.[2]

Fact: Mandating Voter-Verified Paper Trails Could Deny Voters With Disabilities the Right to Cast a Secret Ballot

For the first time, the Help America Vote Act recognized that voters with disabilities should have the same opportunities to cast a secret ballot as everyone else. One key reason for the growth in use of DREs is that they can give everyone a truly private vote; particularly the visually impaired, those with motor skill impairments, or other people with disabilities. For blind or visually impaired voters, including many elderly voters, the creation of a paper trail obviously offers no benefit (causing them, instead, even greater concerns over privacy). Proponents of voter-verified paper trails attempt to respond to the concerns of blind voters by suggesting that they be allowed to verify their ballots, in lieu of paper, by having the DRE read or display their choices back to them prior to final casting of the ballot.[3] Yet this "solution" for the blind is exactly the kind of verification that the law *already requires*, for *every* voter. Apparently such proponents believe that the current technology for ballot verification is fundamentally flawed, yet is somehow still good enough for people with disabilities.

Fact: Voter-Verified Paper Trails In DREs Are An Untested And Unproven Technology

Right now, there are no DRE machines that produce a voter verified paper trail in wide use anywhere in the world. In a recent October 2002 trial of this new technology in Sacramento, CA, for example, printers jammed, and the ballots had to be handled with "many creative tools that were on hand . . . such as a windshield wiper or a back scratcher." Such breakdowns require entire machines be taken out for service, taxing poll workers and creating long lines at the polls. Vendors are working to create new DREs that produce voter verified paper ballots that meet secrecy and security concerns, but these new machines have mostly not been certified by testing agencies and have not been tested in the field.

Fact: Voter-Verified Paper Trails Are of Questionable Value from a Security Standpoint

A piece of paper that shows the voter what they are voting for does not necessarily ensure a secure vote, because assuming a DRE can be rigged, what a paper receipt shows and what the machine counts could *still* be two different things. A better way to ensure accuracy, in addition to rigorous pre- and post-election testing, is to randomly take machines offline during election day and vote on them numerous times to ensure that votes are being counted correctly, a procedure known as parallel testing.

Fact: Voter-Verified Paper Trails Would Create New, Unintended Security Concerns

Producing a paper record creates privacy concerns, as strong security measures would need to be taken to ensure that voters could not take the paper receipts with them upon leaving the polls – opening the door to the sale or even coercion of votes – or that poll workers or elections officials could not violate the sanctity of secret ballots. Keeping a voter's vote secret is critical to a free and fair democracy.

The Leadership Conference on Civil Rights is deeply concerned about the sanctity and security of elections, as the right to vote – and have that vote counted – stands out as perhaps the most important civil right of all. Bearing this in mind, documented improvements in election systems should not be delayed based on unwarranted fears, untested theories, and technology that simply does not exist.

---

[2] To date, there has been no proven instance of attempted fraud in the use of DRE voting equipment. *See* Secretary of State's Ad Hoc Touch Screen Task Force, *Report to the Secretary of State*, CA Secretary of State Kevin Shelley, July 1, 2003, at 18.

[3] Avante International Technology, Inc., *"Response to the 'limitations' of printers (the real story),"* May 6, 2003, http://www.aitechnology.com/votetrakker2/News%20Releases/Response%20to%20Doug%20Lewis%20re%20printers.pdf at 6.

ADVERTISING

NW stock contest 2004
Now through Dec. 31, sign up to play in our annual stock-picking contest. Winner gets lunch on us.

Boeing
Sign up
Boeing e-
newslette

Weekly interest and loan rates | Northwest stock contest 20
Tax tips | Consumer affairs | Home values

Electronic-voting firm reveals hacker break-in

By Monica Soto Ouchi
Seattle Times technology reporter

E-mail this article
Print this article
Search archive

Bellevue-based VoteHere, which sells software designed to make electronic voting more secure, said yesterday a hacker it thinks was politically motivated broke into its computer system and stole nonsensitive internal documents.

The break-in occurred in October but was only publicly acknowle yesterday by Chief Executive Jim Adler.

The incident occurred after the hacker exploited a vulnerability in company's corporate software. VoteHere was "a couple days bef updating a security patch, spokeswoman Stacey Fields said.

VoteHere said it identified the hacker within 24 hours of the breal that it believes the person is affiliated with anti-electronic voting organizations.

The Washington Cyber Crime Task Force — an affiliation of FBI, Secret Service and local law enforcement — is investigating.

No one has been arrested, Fields said.

The breach comes amid growing concern about the security and of electronic voting.

Bev Harris, who runs a small Renton public-relations firm, helped citizens and computer scientists concerned with the potential for fraud after earlier this year discovering an open, unprotected We

112

ADVERTISING

ADVERTIS

Electronic-voting firm reveals hacker break-in

By Monica Soto Ouchi
Seattle Times technology reporter

E-mail this article
Print this article
Search archive

Bellevue-based VoteHere, which sells software designed to make electronic voting more secure, said yesterday a hacker it thinks was politically motivated broke into its computer system and stole nonsensitive internal documents.

The break-in occurred in October but was only publicly acknowledged yesterday by Chief Executive Jim Adler.

The incident occurred after the hacker exploited a vulnerability in the company's corporate software. VoteHere was "a couple days behind" updating a security patch, spokeswoman Stacey Fields said.

VoteHere said it identified the hacker within 24 hours of the break-in and that it believes the person is affiliated with anti-electronic voting organizations.

The Washington Cyber Crime Task Force — an affiliation of FBI, U.S. Secret Service and local law enforcement — is investigating.

No one has been arrested, Fields said.

The breach comes amid growing concern about the security and reliability of electronic voting.

Bev Harris, who runs a small Renton public-relations firm, helped energize citizens and computer scientists concerned with the potential for election fraud after earlier this year discovering an open, unprotected Web site that

113

revealed source code for Diebold voting machines.

The most vocal opponents have called for electronic-voting systems to be backed up by voter-verifiable paper audit trails, a move adopted by California's secretary of state.

VoteHere sells two electronic-voting products. One, encryption-security software for electronic-voting machines, detects when ballots are compromised by adding, deleting or changing a vote.

The other is Internet voting software for private and public elections.

Adler said the hacker didn't access sensitive materials because the company's business model rests upon releasing its source code for all to see.

VoteHere deploys the same encryption technology used to keep credit-card data private during online transactions. The secret is the "key data," a 10-digit number that unlocks the information.

"We're a bunch of cryptographers that decided all the algorithms must be public for the system to be trustworthy," Adler said.

"There's no secret in any of this."

VoteHere released some of its source code earlier this year to be scrutinized by VerifiedVoting.org, a grass-roots organization pressing for accountability in election systems.

David Dill, the group's founder and a Stanford University computer-science professor, said he has yet to find a volunteer with the expertise to verify the company's systems.

"What I think we need, before I'm confident in a system like VoteHere, is a near consensus among experts in cryptography and election administration that the system is trustworthy," Dill said.

"At this point, people haven't looked at it enough to gain a consensus."

Monica Soto Ouchi: 206-515-5632 or msoto@seattletimes.com

Copyright © 2003 The Seattle Times Company

More business & technology headlines

seattletimes.com home
Home delivery | Contact us | Search archive | Site map | Low-graphic
NWclassifieds | NWsource | Advertising info | The Seattle Times Company

Copyright © 2003 The Seattle Times Company

↑ **Back to top**

114

THE Marion Star
OF CENTRAL OHIO

Tuesday, December 30, 2003

Local News

SUBSCRIBE TO THE MARION STAR

Paper receipts proposed to ens accuracy

AP

CLEVELAND (AP) -- A slip of paper is creating a debate in the s voting machines.

The debate concerns whether voters should be allowed to see a ballot before it is cast.

The receipt -- called a voter-verified audit trail -- would then be p box that could be physically counted if results are in dispute.

David Dill, professor of computer science at Stanford University, to fair elections in the electronic age.

"Since there is no way to make sure that the computers are hon free, we can't be trusting any computer count that can't be indep said.

The replacement of punch-card and lever voting machines with e machines was laid out under the Help America Vote Act that foll Gore presidential contest of 2000.

U.S. Rep. Marcy Kaptur, D-Toledo, said many of her constituent electronic machines.

Kaptur and a fellow Toledo Democrat, state Sen. Teresa Fedor, mandate a verified paper trail in Ohio.

Ohio Secretary of State Ken Blackwell has not taken a position c spokesman Carlo LoParo said.

Blackwell has halted the sale of electronic voting machines to c while security issues discovered during a statewide review are a

He has assured that machines certified for sale in Ohio comply w Vote Act, which requires that a paper backup of each ballot cast have closed.

LoParo said no machine certified for use in Ohio is equipped to f

115

each voter. He said the machines' manufacturers could install such a system, but it would increase the cost by up to 25 percent.

Blackwell believes optical-scan machines could be used as an alternative. Voters fill out a ballot card by hand and insert them in optical-scan machines, which read pencil marks next to their selections and automatically tabulate results.

The machines are designed to eliminate overvotes for the same office that punch-card and lever systems don't always catch. They can be designed to refuse to accept ballots with errors and allow voters to recast them.

But Lloyd Leonard, national advocacy director for the League of Women Voters, said any kind of paper system has risks.

"If there is a moral to the Florida story from 2000, it's that paper ballots are insecure and unreliable," Leonard said. "So it seems strange to us to want to enshrine a paper ballot system."

Email this story

Originally published Tuesday, December 30, 2003

Contact Us | Subscribe | Place an ad
Copyright ©2003 The Marion Star. All rights reserved.
Use of this site indicates your agreement to the Terms of Service
(Terms updated 12/20/02)

116

Don't let his hero's smile fool you, he is *all business!* Goldey-Beac (302) 225-6248 Bachelor Degree or Master of Business Administration

TODAY IS Wednesday, December 31 , 2003

Local News from The News Journal

need help? h

States rethink voting systems

Security problems spark concern over machines

By J.L. MILLER
Dover Bureau reporter
12/25/2003

Concerns about security flaws have prompted officials in four states to re-evaluate their electronic voting systems, with some critics saying new systems put in place after the 2000 Florida election scandal open the door to widespread fraud.

At minimum, critics contend, the new electronic machines should be required to produce a paper receipt of each vote cast that can be kept as a backup in case of equipment failure or disputed results. Most touch-screen electronic systems do not produce a paper record.

Sen. Barbara Boxer, D-Calif., and Rep. Rush Holt, D-N.J., said last week they will introduce a bill requiring electronic voting machines to produce paper records by November 2004 to ensure accurate elections. Manufacturers said that will add hundreds of dollars to the cost of machines.

The move toward electronic voting has been propelled by the federal Help America Vote Act of 2002, which authorized $400 million to states to replace punch-card systems in time for the 2004 presidential election. The law, a response to the Florida dispute after the 2000 presidential vote, also provided $2.5 billion to help states improve existing machines and voter registration technology.

The security concerns focus on machines made by Diebold Election Systems, Election Systems & Software, Hart InterCivic and Sequoia Voting Systems. Their machines are subject to various security flaws, according to an independent review commissioned by the state of Ohio. Ohio, California, Maryland and Nevada are the four states re-evaluating their electronic voting systems.

Researchers at Johns Hopkins University said in August the security measures employed in Diebold voting machines - which will be used in Maryland's primary elections in March - are "far below even the most minimal security standards applicable in other contexts."

So far, Delaware's computerized voting system has remained largely free of criticism.

Older machines less risky

The Danaher machines Delaware switched to in 1998 use older technology that appears to be less vulnerable to tampering than newer systems. The Ohio and Johns Hopkins studies did not review Danaher machines.

"We look better each day when these reports come out," Elections Commissioner Frank B. Calio said.

ELECTRONIC VOTING

1. Machines are kept unc
a seal that will show if th
tampered with. Before th
to the polling places, the
each county certifies thal
the vote-counter on the l
set at zero.

2. When the machines ai
places, the seals are brol
workers view the backs c
make sure the tally still r

3. Voters submit identific
eligible to vote. Their nai
and they are directed to

4. The ballot is displayed
blinking red light identifie
on the ballot. Voters pres
the candidate's name an
off. When all the red ligh
offices have been voted.

5. The voter presses a re
below the ballot marked
recorded on a removable
of the machine, and on a
machine.

6. When the polls close,
taken to state offices call
one zone in Kent County,
eight in New Castle. The
into a reader, and the re
to the Election Commissi
the state's mainframe co
are tabulated and placed
come in.

7. Two days after the ele
and the paper tapes are
Canvass in each county,
reviewed and certified.

U.S. & World News >>
updated every 30 minutes

SPONSORS

117

The city of Philadelphia in its last four elections has used the Danaher machines, which have performed well, according to Fred Voigt, executive director of the nonpartisan watchdog group the Committee of Seventy.

Diebold machines, and other newer models in other states, employ operating systems akin to those that run personal computers. Security experts found that code in those machines could be rewritten to disrupt elections or alter the results.

Some of the affected machines are connected to modems and telephone lines, opening an avenue for hackers. The codes that run some of the machines have been widely circulated on the Internet, giving hackers opportunity to rewrite them.

The Diebold machines also use electronic "smart cards" that are issued to voters, who place them in the voting machine to cast their votes. But blank smart cards are available from computer supply companies, and an enterprising hacker could program one to record multiple votes for chosen candidates.

Bev Harris of Renton, Wash., author of "Black Box Voting: Ballot-Tampering in the 21st Century," said it was difficult to rig large numbers of mechanical voting machines, but electronic machines are different.

"It doesn't take very many people. It takes just one to slide in a replacement program," Harris said.

Harris said assurances that multiple memory tables and backup paper tapes will ensure accurate election counts miss the real point: There is no way for the voter to verify that the machine has recorded his ballot correctly. The machines do not print a receipt showing each vote.

Critics suggest electronic machines need to print out a receipt of each vote. The receipt then could be dropped into a ballot box to serve as a backup, and allow for an audit.

Tampering would be more difficult with the Danaher electronic machines Delaware purchased in 1998 to replace its mechanical voting machines.

They do not have operating systems with code that can be altered, according to Calio and Matthew Lilly, vice president for sales and operations for Danaher's voting-machine business. Instead, the instructions that run the machine reside on computer chips.

"You can't get access to it, you can't change it. It is embedded in the equipment, and it cannot be altered," Lilly said.

Philadelphia's Voigt said the security of the Danaher machines was one factor his panel examined. Even if someone could successfully reprogram a Danaher machine, Voigt said, the programmer would have to know in advance all the names on the ballot and the order in which they would appear.

The votes are recorded on paper tapes and on a removable cartridge that is downloaded directly into the state's mainframe computer, which cannot be accessed from outside the system. The machines are not hooked to phone lines and do not have modems.

Although the Danaher machines have performed well in Delaware, there have been occasional problems elsewhere. The machines used in Delaware have proved accurate enough that the losers of two close state House races in 2002 did not ask for recounts. One of those was Shirley Price, a Democratic state representative from Millville, who lost her seat to Republican Gerald W. Hocker by just 57 votes. "I think that they are much more accurate and there's less opportunity for error," Price said. "That certainly was a key factor in my decision not to ask for a recount."

LEISURE
THE EQUIPM
www.leisure
NEW
NEW
LEISURE
THE EQUIPM
www.leisure
CLICK HERE
800-499
FOR LOC

ESSENTIALS
- Weather
- Traffic
- Obituaries
- Celebrations
- Government
- Births
- Lottery
- Police news

118

Sign up for mySunSpot to get these new
>> Breaking news >> Weekly update >> A&E >> Eats >>

Voting device debut in Md. is uneventful

Poll workers around state report no large glitches in municipal elections

By Stephanie Desmon
Sun Staff
Originally published November 5, 2003

A handful of Maryland municipalities welcomed voters to the polls yesterday, some providing a first look at the touch-screen voting machines set to be the future of elections statewide.

Cities and towns reported no major glitches with the machines made by Diebold Election Systems, which have been criticized as being vulnerable to hackers and tampering. Yet the day did not pass without some dispute, as members of the newly formed Campaign for Verifiable Voting handed out fliers protesting their use.

"There is a lot of concern about this," said Kevin Zeese, a Takoma Park attorney leading the protest. His biggest complaint is that a traditional recount cannot be conducted because there is no paper trail once a vote is cast. Using these machines, he said, a recount would involve pushing the same button and recording the same number.

Four counties used the machines during last year's gubernatorial election. Two more - Kent and Wicomico on the Eastern Shore - used them for the first time yesterday.

The rest of the state's counties are expected to have them in time for the presidential primary next spring. Baltimore, which uses a different type of electronic machine, is expected to have the new ones installed by 2006. The state is spending $55.6 million to install the devices.

In July, a team of researchers based at the Johns Hopkins University concluded that the underlying computer code in Diebold's machines could be vulnerable to tampering. Gov. Robert L. Ehrlich Jr. then ordered another review, which found the system "at high risk of compromise." But purchase of the machines will continue, officials said.

Yesterday marked the machines' debut in Salisbury, where voters

119

site
We make it easy.

Quick search
Type search term(s) for articles, places or events, then hit enter

were choosing three City Council members. By midday, City Clerk Brenda Cogsgrove said turnout appeared to be ahead of September's primary, when 24.1 percent of 8,000 registered voters cast ballots using optical scanners.

"I was out this morning giving demonstrations on the new system for elderly voters or anybody who needed it," Cogsgrove said. "Everything seems to have gone very smoothly - no problems, no complaints."

Officials in Chestertown, Rockville and Gaithersburg also reported a smooth day. "So far, so good," said Mary Beth Smith, a spokeswoman for the city of Gaithersburg.

Sun staff writer Chris Guy contributed to this article.

Copyright © 2003, The Baltimore Sun | Get home delivery

(5:08 I

Deal shap
Many House statew

Man from wins
Newly counc so ma suppo

sunspot.net

Talk about it Discuss this story | **E-mail it** Send this story to a friend | **Print it** Printer-friendly version | **Co** Se

Maryland | Nation/World | Education | Health | Obituaries | Traffic | Weather | Lottery | AP News
News | Business | Sports | Arts/Life | Opinion | Marketplace

Contact us: Submit feedback, send a letter to the editor, submit a news tip, get subscription info, or place a classified ad.

www.sunspot.net (R) and baltimoresun.com (TM) are copyright © 2003 by The Baltimore Sun.
Terms of Service | Privacy Policy

MERCED SUN-STAR.com

Merced Weather
Temperature: 61 °F
Humidity: 37%
Wind speed: 6 mph
View Radar | Ho

Wednesday, November 05, 2003

"Gatewa

READER POLL

Was John Headding the real reason behind the problems at Mercy Medical Center Merced, or just a scapegoat?

The real reason.

Just a scapegoat.

Vote Now!

Total Votes: 67

View Results

SEARCH

Search for:

Go

NEWS
- City/County
- Schools
- UC Merced
- Health Care
- Politics
- Crime & Courts
- Police calls
- Local Briefs

SPORTS
- Merced College
- Prep Sports
- Where Are They Now?
- Local motorsports
- All-Area Selections
- Prep Football

LIFESTYLE
- Crossword puzzle
- Food, Dining, Recipes
- Genealogy
- Health, Food Notes
- Merced History
- Milestones
- Pets

Officials say touch screen voting system passed test

Wednesday, November 05, 2003

By Cheri Carlson - Merced Sun-Star

Despite a power outage affecting a handful of polling precincts in Merced, county election officials say that months of preparations paid off Tuesday and the county's introduction to touch screen voting was a success.

Photo by Marci Stenberg

Jan Weiss elections volunteer, right, shows Li Thao, front left, and Pao Chang the process of using the voting machine at the Merced County Administration Building on 22nd and M Street Tuesday morning.

Aside from the disappointing voter turnout - which late Tuesday night was reported at about 20 percent - Merced County Auditor/Controller Steve Jones said the county transitioned well into its first paper-free election.

"We've been tested in every avenue," he said. And, "things have run pretty smoothly."

A few minor problems popped up early in the day, according to Jones, but were cleared up right away.

The biggest potential challenge Tuesday was sparked by the power outage affecting North Merced.

"If we didn't have these (new) machines we would have been in trouble," said Jones.

The batteries, which are guaranteed for six hours, were swapped at a half-dozen precincts that remained without power for most of the day.

Photo by Marci Stenberg

Spencer Puita, 17 months, watches as his father Rick casts his votes Tuesday morning in the American Legion Hall on Main Street.

Other problems included a mix-up in Atwater where a couple voters were unable to vote on a particular race, although details about that incident weren't clear Tuesday night. The problem was reported within the first hour of the polls being opened, and Jones said the voters were contacted and came back later in the day.

Another polling place in the Weaver School area wasn't open for poll workers

TODAY'S F

Click

BIG VALLE CLASSIFIE
- Place an
- BV Class
- New BV Registrat
- Announc
- Apartme
- Automot
- Boats
- Farm/Ag
- Garage/
- Homeow
- Job Trair
- Jobs
- Merchan
- Mobile H
- Personal
- Pets
- Real Est

DO YOU USE GROCE COUPON

For G News

Merced

- Religion
- Reunions
- Seniors
- Sun-Stardate
- 411 for Teens

OBITUARIES

BUSINESS
- Agriculture
- Food & Farm News

OPINION
- Sun-Star Editorials
- Letters-to-the-Editor
- Guest Perspectives
- The RED PHONE

CANDIDATES ON THE ISSUES

Several local elections will be decided Nov. 4. In a new special section, the Merced Sun-Star grills the individual candidates on issues our community faces. See the new "Candidates on the Issues" under "Special Sections" below, and then vote informed on Nov. 4.

SPECIAL SECTIONS

- Merced at Work
- Reference Desk
- Poetry Section
- Candidates on the Issues
- Heroes 2003
- Turlock Journal
- Home Improvement
- Merced County Fair 2003

COMICS/CARTOONS

- Editorial Cartoons
- PHIL & J.T.

MARKETPLACE

- Advertisers
- Big Valley Autos
- Big Valley Churches
- Big Valley Health
- Big Valley Retail
- Big Valley Tech
- Entertainment Guide

Tuesday morning, but Jones said the miscommunication was quickly resolved and the precinct opened shortly after 7 a.m. One voter, who showed up when the polls opened, was able to wait through the short delay, Jones added.

Overall, everything went well, reported election officials, who said that feedback from voters regarding the new system was positive.

In July, the county's Board of Supervisors approved a contract with Elections Systems & Software to update the county's voter registration and election equipment.

The $2.1 million voting system - which includes touch screens and audio equipment in English and Spanish - is designed to make voting easier for the deaf and blind.

Janette Stevens, who has low vision, was able to make use of that feature Tuesday.

Instead of having to see or have someone help her read the ballot, she could listen to the machine.

"It made it much easier," she said Tuesday night.

Her mother came with her to vote at the County Administration Building and also gave the new machines a good review.

"It was much clearer," said Melba Stamper. "More user-friendly."

Election results are available at www.co.merced.ca.us.

Reporter Cheri Carlson can be reached at 385-2477 or ccarlson@mercedsun-star.com.

E-mail this article to a friend | **Printer friendly format**

SUBSCRIB

Get our fre newsletter enter ema

ENTERTAI
- Arts
- Books
- Food
- Movies
- Skatebo
- Wineries

COMMUNI
- Merced C semester

PHOTO GA
- Photos f
- Photos f 2003
- Photos f 2003
- Photos f 2003
- Photos f 2003
- Photos f 2003

More Ph

COLUMNIS
- ANDRE

CLEAR
33°
more weather

My child needs a hearing exam.
Where should we go?
Toledo PROS
Making a Difference
Advertisement

SEARCH
Search by keyword(s):
go
Tips on searching

ARCHIVES
Browse Last 30 Days
The Blade Archives
AP Archives

NEWS SECTIONS
Latest News
Opinion
Sports
Business
Arts & Entertainment
Davis-Besse In-depth
Religion
Science/Tech
Columnists
Obituaries
Special Reports
Weather
AP Wire
Photos of the Day
Lottery
Daily Log
Today's Front Page

CLASSIFIED
General
Real Estate
Autos
Jobs
Boats/Recreation
Celebrations
Legal Notices
Directory of Worship
Personals

COMMUNITY
Golf Guide
Restaurant Guide
Arts/Events Calendar
Educational Services
Forums

Elections | Article published Friday, December 26, 2003

Kaptur: Voting system still needs work

By FRITZ WENZEL
BLADE POLITICAL WRITER

Security flaws found in voting machines earmarked for use in Ohio should be remedied quickly, making the machines available to county boards of election by early spring, a top aide to Secretary of State Kenneth Blackwell said this week.

Carlo LoParo, spokesman for Mr. Blackwell, said once fixes are made, "most if not all" of the equipment offered by the four election equipment makers approved to sell their machines in Ohio under a new federal election reform law will have to go through a new round of federal and state certifications.

But fixing those flaws remains just part of the job some Democrats, including U.S. Rep. Marcy Kaptur (D., Toledo), say needs to be done to see that elections are honest and fair.

They have called for modifications to voting hardware and public scrutiny to voting software to make it more transparent.

The veracity of computerized voting equipment, once a lonely topic left to elections insiders, is developing into a national issue with bitter partisan implications.

Counties nationwide are replacing their old mechanical lever and punch-card voting machines to comply with a federal election reform law passed last year. The Help America Vote Act was adopted to guarantee there would never be another presidential election debacle like that in Florida, 2000.

Billions in federal money are at stake, and the voting machine industry has blossomed, with many companies offering their own version of computerized touch-screen voting equipment, each run with an internal computer.

The security of the computer software has been at the center of a national controversy, fed earlier this month by a report from Secretary Blackwell's office that determined the systems of Ohio's approved vendors had potential security flaws that needed to be fixed.

Lucas County has tentatively selected the equipment manufactured by Diebold Elections Systems of North Canton, Ohio, and has used its equipment in two elections.

To Miss Kaptur, the issue has taken on such a heavy partisan slant in favor of Republicans - who have majorities in the state legislature and Congress - that she has begun speaking out.

E-thepeople
TV Listings
Movie Showtimes
Horoscopes
WEB FEATURES
Toledo Pros
HBA Parade of Homes
toledo
Contests
Mud Hens Web Cam
SERVICES
Set As Homepage
Subscriber Services
Email Newsletter
The Blade e-edition
Advertise
About Us
Contact Us
Help & FAQs

She voiced concern again this week that Diebold may be getting preferential treatment in the process because its officers have given heavily to Republicans.

"If you permit private companies [into the process] like Diebold that have made huge contributions to the Republican Party in this state and nationally, you give these private interests a leg up on the general public. Our job in the public realm has to keep those private interests at bay, and represent the public's interests first," she said.

"Elections belong to everyone, they don't belong just to those who know how to make the machines or program the machines," Miss Kaptur added. She has called for voting machine companies to make public their proprietary computer programming codes to allow the public to inspect them for possible defects.

She stopped short of accusing Diebold of using their software to fix elections, but she said, "They have that capability."

And she charged Tuesday that Secretary Blackwell, a Republican, has appointed a secretive committee of GOP supporters to negotiate contract language with election machinery companies and oversee installation of the new high-tech voting devices.

"When you take something a little more sophisticated out of the hands of the general public, it becomes less democratic. And therefore, you have to work harder to make sure that those involved are equally balanced from a partisan standpoint," she said. "We certainly haven't had that in Ohio."

Mr. LoParo sharply disputes the Kaptur claims.

"That's an unfortunate accusation without basis," he said. "One would expect better from a member of the United States Congress than to throw out inaccurate accusations simply to incite and to cast doubt on a process that has been the most open and transparent in the country thus far."

"She should be ashamed of herself," he said.

"Across the board this has been a bipartisan process that has included individuals based on expertise and the value that they bring to the process. If Miss Kaptur doesn't understand that, that's just unfortunate," he added.

Two of the seven members of the Blackwell committee are Democrats who have held statewide offices in Iowa and Massachusetts, he said.

Mark Radke, director of marketing for Diebold, said independent testing of his firm's equipment has shown that not only is tampering to produce partisan advantage nearly impossible, it could be detected and exposed.

Diebold has come under fire in part because its chairman, Walden O'Dell, circulated a fund-raising letter earlier this year declaring that he wanted to deliver Ohio's electoral votes for President Bush in next year's election. He has apologized for the letter because it didn't clearly separate his personal political agenda from his association with the voting machine company.

"Mr. O'Dell is one of 13,000 employees at Diebold, and each employee, because of this democratic society, has their own free will to have their preferences ... as far as their political party," Mr. Radke said.

"We have gone through two full evaluations of our software code and the overall functionality of our equipment," Mr. Radke said. "The entire Compuware and Info Sentry [security] reports were made public, so there was nothing hidden from

Strabler
HEARIN
Hearing
HEATIN
CONDIT
Shamy
Conditic
HOME M
EQUITY
Midwest
Investm
INVEST
RETIREI
& FINAN
America
Financia
PERSON
MALPRA
Barkan
PLASTIC
Arrowhe
Surgeon
PLUMBI
CONTRA
The Cle
REAL ES
APPRAIS
Contine
REAL ES
AUCTIO
Beth Ro
REALTO
Char Wi
Re/Max
Makin

124

anyone about the overall evaluation of our system."

Those evaluations are posted online at Secretary Blackwell's Web site.

In a related development, state Sen. Teresa Fedor and state Rep. Peter Ujvagi have introduced legislation requiring touch-screen voting machines to have printers that can produce paper receipts for voters to inspect before they leave the polls. The bill is designed to boost voters' confidence that their ballot will be counted properly.

More articles on this subject »

Commission seat races take shape 12/26/2003
Mich. lawmakers OK elections overhaul 12/19/2003
School-fund issues top primary ballots 12/19/2003
Issues abound on March ballot 12/19/2003
Commission rejects campaign complaint 12/17/2003

More »

Article Features »

Printer-friendly version
Email to a friend
Forum on this topic
View the Latest News index

Subcategories »

2002 Census	Environment	Police
America Remembers	Fires	Politics
Davis-Besse	Higher Education	Regional News
Lucas County	K-12 Education	Religion
Medical/Health	Michigan News	Suburban News
Accidents/Vehicular	Minority Issues	Transportation
City of Toledo	Obituaries - News	War on Terrorism
Courts	Ohio News	Weather
Elections	Other	Zoo/Library/Museum

© 2003 The Blade. Privacy Statement. By using this service, you accept the terms of our visitor agreement. Please read it.

The Toledo Blade Company, 541 N. Superior St., Toledo, OH 43660, (419) 724-6000
To contact a specific department or an individual person, click here.

125

The Clarion-Ledger MISSISSIPPI NEWS
clarionledger.com REAL MISSISSIPPI

November 6, 2003

Errors hold up Hinds results

By Sylvain Metz
smetz@clarionledger.com

The counting in Hinds County will start up again this morning, two days after voters cast ballots.

Hinds County Election Commission members must count 2,584 affidavit ballots, 1,400-plus absentee ballots and "Lord knows how many paper ballots, probably a couple of thousand," said District 4 Election Commissioner Connie Cochran.

"We paid $1.6 million for voting machines and hundreds of thousands of dollars on training" and the results are still unknown, said Hinds County Tax Assessor Bill Burrow Jr., who was trailing Democrat Eddie J. Fair in a re-election bid.

A number of electronic, paper and affidavit ballots had yet to be counted in all the Hinds County races, but only one remains too close to call. Republican Sen. Richard White, a 13-year incumbent, held a 49-vote lead over Democratic challenger Dewayne Thomas on Wednesday.

As many as three dozen voting machines were unexpectedly left at precincts overnight. "Somebody dropped the ball," said Cochran, who, with other members, attributed the snafu to overwhelmed poll workers who went home after a long day. By noon Wednesday, 31 machines were still outstanding. All machines were returned Wednesday afternoon and tallied.

Election Commission Chairwoman Lelia G. Rhodes could not predict how many votes were yet to be counted.

In 1999, an estimated 66,000 people voted. Incomplete numbers indicate 59,000 people cast ballots Tuesday, according to Circuit Clerk Barbara Dunn. About 878,000 voted statewide.

Rhodes and Cochran admitted there were problems — voting machines that overheated, a lack of paper ballots for voters to use when machines went down, and the long waits in line.

Pete Perry of Jackson saw the flaws in how Tuesday's election was handled. Perry, a political buff who visited more than 80 precincts around the county

Tuesday, said there appeared to be a lack of machines at busier precincts.

At one polling place, where he said 600 signed in to vote, there were only two machines. At another, where 178 voted, there were four machines. And in another, where he found between 1,200 and 1,300 people signed in to vote, there were five voting machines.

Hollis Watkins of Jackson, one of Fair's supporters, defended commission members. "I think the process is a good one," he said. "We need to let them complete the process."

Statewide, officials reported few voting irregularities. Secretary of State Eric Clark has sent letters to the U.S. Attorney's office and the state attorney general's office listing problems.

Clark pointed out that poll workers in Lowndes County allegedly videotaped voters in largely minority precincts. In Canton, there were reports of poll watchers attempting to follow voters into polling booths.

Mississippians with complaints about Tuesday's elections should contact the state attorney general's office, said Nancy East, spokeswoman for Attorney General Mike Moore.

Staff writer Andy Kanengiser contributed to this report.

Send this article as a postcard

Copyright © 2003. The Clarion-Ledger.
Use of this site signifies your agreement to the Terms of Service. We welcome your comments. E-mail us.

127

washingtonpost.com Personalize Your Post | Go to mywashingt
Home News Politics Entertainment Live Discussions Photos Marketplace Jobs
▼ADVERTISING
Navigate to Sections GO SEARCH: News GO Search Op

Voting Machine Glitches Prompt GOP Challenge

Eric M. Weiss and David Cho
Washington Post Staff Writers
Tuesday, November 4, 2003; 11:52 PM

Widespread problems with new touch-screen voting machines delayed election results in Fairfax County Tuesday night and led to a legal challenge by Republican officials.

▼ADVERTISING Nine malfunctioning voting machines were removed for repair and then put back in service, a move that Fairfax Republicans said broke election law. Several hundred votes were under scrutiny, not enough to affect the outcome of county-wide races.

A circuit court judge will hear arguments Wednesday morning on whether those votes should be set aside.

The new machines, meant to simplify voting, made the tallying of the votes more problematic, with more than half of precinct officials resorting to the old-fashioned telephone to call in their numbers or even driving the results to headquarters, elections officials said. A handful of precincts resorted to paper ballots.

Election officials said it was the slowest performance in memory for counting votes on election night in the county. The problem came when precinct workers tried to electronically send results from the 953 new machines to election headquarters, unexpectedly overloading computer servers.

When the electronic system of sending results over telephone modems failed, precinct workers tried to call in the results but were met with busy signals. Many decided it would be quicker to drive.

Some voters also complained about using the new machines, and officials said that resulted in slow going at some polling places during the day. For example, a line of 100 people snaked around the polling room at Sleepy Hollow Elementary School Tuesday morning, workers said.

Fairfax election officials expressed surprise at the glitches.

"I don't know what the holdup is," Margaret K. Luca (D), secretary of the county's three-person elections board, said late Tuesday night. "I thought we had it covered. We tested all week in the county."

WASHINGTON ARE
Virginia House of De
Virginia State Senate
Maryland
Virginia
——Multimedi
• Va. Voters Head to Pc
Washington Post reporter
reports on voting in Fairfa
• Fairfax Frontrunners:
County candidates Gerald
(D) and Mychele B. Brickr
for votes in the race to be
chairman of the county's
Supervisors.
——Voters Guic
• N.Va. Voters Guide: R
the candidates running in
2003 elections.
——Full Covera
• 2003 Va. Elections
——Free E-mail New
• News Headlines
• News Alert
E-Mail This Article
Printer-Friendly V
Permission to Rep
Subscribe to The

128

Fairfax spent $3.5 million on 1,000 WINvote machines this year, part of a wave of new technology being introduced to voting booths in the wake of the ballot-booth drama of the 2000 presidential election. The machines, made by Advanced Voting Solutions of Frisco, Tex., resemble laptop computers without keyboards.

Fairfax and Arlington used the technology countywide for the first time Tuesday. Arlington reported no major problems.

The most serious complaints in Fairfax centered on the several hundred votes tabulated by nine problem machines across the county.

A hastily filed lawsuit by the Fairfax County Republican Committee and Friends of Mychele Brickner (R), the losing candidate for board chairman, asks the court to set aside the votes from the nine machines until a judge determines whether they were recorded properly.

Circuit Court Judge Dennis J. Smith agreed to hear the motion this morning.

The nine machines were located in the following precincts: Floris, Dulles, Kenmore, Freedom Hill, Kilmer, Waynewood, Reston 1, Rose Hill and Masonville, according to the lawsuit.

"It is our information that there are irregularities," said Christopher T. Craig, attorney for the Republicans. "Voting machines were moved out of polling places and back into the polling places, and they are not supposed to be. That is not supposed to happen."

Craig said election law prohibits the removal of machines in the middle of voting.

Luca said there were "unanticipated problems" with the nine machines. Election workers in the nine precincts tried to reboot the machines as trained, she said, but that did not solve the problem. She then decided it would be best to bring the machines to the county government center, where technicians were better prepared to deal with them.

"The whole idea behind these machines is that they are portable, so it made more sense to bring them to where you had the technology and the people to fix . . . these problems," Luca said.

Craig acknowledged that the number of votes, estimated in the hundreds, "may not make any difference, but that is not the point."

"It's about voter integrity," he said.

In Montgomery County elections in September 2002, electronic voting machines were blamed for confusion. Several polling places opened late because the equipment was not set up, and inaccurate results were posted on the county Web site while judges struggled through complicated forms and

THE JOURNALNET
thejournalnet.com

Last Updated: Tuesday, November 04, 2003 11:51:00 PM

▶ News

Print this article E-mail this article

Johnson County embraces touchscreen voting

By MATT MILLER
Daily Journal staff writer
mmiller@thejournalnet.com

Nov. 5, 2003

Johnson County said goodbye to hanging chads and debuted new touchscreen voting machines with few technical glitches or confused voters.

Evacuation of a smoky building on Tuesday at one precinct delayed voting for several minutes. At another polling place, a voting machine malfunctioned, but was back in service within minutes, and no votes were lost.

Election staff had most votes tabulated by 8 p.m., more than an hour earlier than in previous elections. Poll workers completed their post-election tasks and headed to the Johnson County Courthouse in a fraction of the time it took with the old punch-card ballots.

Voters took less time, too.

Dennis Wells finished his ballot in less than two minutes at Greenwood Fire Station No. 2 on Fry Road.

An explanation of new machines took 30 seconds. He was done voting less than a minute later.

"It took me more time to find out where to drop off the (instruction) card," the 53-year-old Greenwood resident said.

The county bought 456 of the iVotronic machines, which work like an ATM, for $2.42 million. About 170 were used on Tuesday.

The machines, just larger than a laptop computer, were touted as reliable. They store ballot counts in three separate memory areas. If one memory source fails, two others should be able to back it up.

Having a malfunction in only one machine is a success in any election, said Dan McGinnis, senior vice president of Election Systems and Software, the company that produces the touchscreen machines.

"That's almost no failure rate at all," he said.

Speedy vote tabulating was another selling point for the machines. Cartridges at each precinct collected vote data from the machines, and workers carried them to Election Central. In seconds, the cartridge was inserted into a reader and vote information was added to a master computer.

Master cartridges from all 54 precincts were successfully read and recorded by computers at Election Central at the courthouse. Most of the county's results were done before 7:30 p.m.

If poll workers from one precinct hadn't arrived 30 minutes later than the rest, results would have been done before 8 p.m., County Clerk Brenda Jones-Matthews said.

Most election nights, the staff and poll workers remain at the courthouse until at least 9:30 or 10 p.m. tabulating ballots.

Poll workers underwent two-hour training sessions to help voters to operate the devices. They also were trained on a voting machine that read the ballot to visually impaired voters.

Voters were trained, too. County voting officials offered test sessions where residents could try the iVotronics and ask questions before Election Day.

"A lot of the older ones were saying, 'Cool,'" said Mary Davisson, a clerk at the White River Township Precinct 19.

The new iVotronic election machines went over well with voters at Pleasant Township Precinct 29, in the Greenwood Senior Citizens Center at 550 Polk Ave. in Greenwood.

"I'd say 99 percent of them did just fine," poll worker Rob Shilts said.

Voters using the high-tech voting machines for the first time remarked, "Wow, this is really easy," and "Is this all I have to do?" Shilts recalled.

"Once they've gone through it, they seem to be pretty satisfied," he said. "The nice thing about it is, if people have a problem, they can go back and review the vote."

The iVotronic has a feature that requires voters to review their ballot before casting it and allows them to change their selections before doing so.

But Shilts noted that one voter earlier in the day appeared frustrated by the unfamiliar computer touchscreen ballot. Poll workers explained the procedure, and she was able to cast her vote; but hinted she might

not return next Election Day.

"She said, 'I'm not going to go through that again,'" Shilts said.

With that exception, everyone else at Pleasant 29 breezed through the process. Many already knew the county had retired the old punch-card ballots — made famous by the 2000 Florida presidential recount — and replaced them with electronic voting machines.

"I think one of the biggest things we heard was, 'No more hanging chads?'" Shilts said. "So there were a lot of Florida references and 'hanging chad' references."

Jessie Simpson, a 73-year-old Greenwood resident who voted at Greenwood United Methodist Church, liked the simplicity in changing her responses. With the old punch-card ballots, voters who made a mistake had to request a new card.

Matt Nichols called his experience at the new touchscreen machines efficient, even though he didn't completely agree with county officials' decision to buy them.

"I thought the punch cards worked fine," said Nichols, 31, of Greenwood. "I think they could have spent the money some other way."

In 2004, with elections for president, governor, state representative and several county offices on tap, next year's election will be a bigger test for the iVotronic machines. The last such election, in 2000, brought record numbers of voters to the polls in Johnson County. Officials expect to use all 456 touchscreen machines next year.

After the iVotronic machines' first test in Johnson County, election officials — including a new county clerk — will probably modify a few procedures, Jones-Matthews said.

The most obvious: changing the way that voters check in and out of the polls. Voters were given a laminated card with directions for using the touchscreen machines.

They handed it to poll workers before voting and after they had finished so the workers could ensure votes were cast properly.

The election board will probably find a new, less-confusing way of making sure votes are cast correctly, Jones-Matthews said.

More races and more voters next year will mean that a new clerk will have to hire more staff to work at the polls, Jones-Matthews said.

"It's going to be double everything," she said.

The Miami Herald
Herald.com

Broward

Posted on Tue, Nov. 25, 2003

ELECT-TRONICS

Voting hi-tech safer, costlier

A county report found Broward officials should watch to California does before adding printers to the $17.2 millio machines it bought two years ago.

BY ERIKA BOLSTAD
ebolstad@herald.com

Hi-tech voting costs mount

As the next innovation in voting technology takes hold, County should take a wait-and-see approach, learning fr experience and missteps of others, a new report advises

Commissioners asked in September for an analysis of ac to touch-screen voting machines, so people could see a of their electronic choices.

The report indicates the $17.2 million touch-screen votir used in Broward County is trustworthy, but security proc controls should be continually re-evaluated and strength increase voter confidence.

However, before buying more equipment, Broward Cour watch how California handles a mandate to create paper electronic ballots, said Pete Corwin, the county official w report.

Commissioners requested the study in the midst of grov concern about the security of electronic voting. Miami-D asked for a similar review.

As more counties across the United States upgrade votin what was once a fringe movement among computer scie community activists has entered the mainstream debate election reform.

133

Classifieds
Newspaper Ads
Special Sections
Services
Archives
News by Email
Subscribe
Place an Ad
Site Index
Contact Us
More Herald Services
Partners
El Nuevo Herald
Street
Gay South Florida
Top Vacation Picks
More Partners

"Everybody is rethinking their procedures and everybody is rethinking their testing," Corwin said. ``The good that's coming out of this debate is that you cannot take for granted anything you want secure."

= [100.0] = [100.0] ers or other devices that create a paper trail of individual ballots.

2001 UPGRADE

Broward bought its equipment in late 2001, under pressure to upgrade from punch-cards. That system was outlawed during voting reforms that swept Florida in the wake of the 2000 presidential recount. Fifteen Florida counties use some form of touch-screen equipment. The other 52 use optical-scan equipment, which voters mark with a pencil and election workers run through a machine to counts the marks.

In hindsight, it might have been better to make a more deliberative decision, said Broward County Mayor Ilene Lieberman.

This time around, Broward County can take its time and see what voting-machine manufacturers come up with to address California's needs. Instead of being at the forefront of voting reform, Broward can stand back and watch, Lieberman pointed out.

"I just don't want to be under the gun again," Lieberman said.

2000 DEBACLE

But some county commissioners who have backed a paper trail for voters said they don't want to wait. Voters, especially in Broward, have seen their trust in elections shattered by the 2000 presidential recount and the legacy of suspended Supervisor of Elections Miriam Oliphant, said County Commissioner Lori Parrish.

"I think Florida needs to certify it now," Parrish said. 'I think we need to restore voters' confidence.''

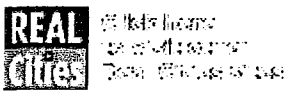
The county report also finds that if the county were to ditch its sophisticated touch-screens in favor of optical-scan equipment with paper ballots, elections might not be any less expensive.

While touch-screen machines must be carefully stored, programmed and transported to polling places, an optical-scan system requires paper ballots, which also are expensive.

At 25 cents a page, a three-page ballot for a general election would cost about $750,000, the report found.

email this | print this | license this | reprint this

134



News | Business | Sports | Entertainment | Tropical Life | City Guide | Shopping | Jobs | Cars
About Herald.com | About the Real Cities Network | Terms of Use & Privacy Statement | About
Copyright

TECHNOLOGY ADVICE YOU CAN TRUST

PCWORLD

> > >

Controversy surrounds new e-voting systems set for wide use in 2004 elections.

Janet Rae-Dupree
From the February 2004 issue of PC World magazine
Posted Monday, January 05, 2004

This election year, rather than punching holes or connecting dots on paper ballots, many of us will cast our votes on electronic touch screens.

Electronic voting systems are already in place in eight states and were used in last November's elections. Many more states will use them in this year's primaries and in the presidential election. Good news, right? After all, computers have to be more accurate and less subject to fraud than old chad-prone paper ballots--don't they?

Critics say no, claiming that there are numerous problems with oversight and monitoring of the electronic election process. But change is already under way, including several federal bills that would require some form of permanent and immediate ballot trail, and better security.

At Your Fingertips

The actual e-voting process is simple. Before entering the booth, voters receive a unique identifier (a smart card programmed for single use, for example, or a randomly generated number) to activate the process and make sure only one ballot is cast. At the booth, voters typically see an ATM-like interactive screen with candidates' names; then they touch the screen to make a selection--the computer does not let them choose too many. When they're done, voters see a summary screen with their choices, accept it, and press an icon to end their session.

The machines store votes on removable PC cards, where they stay until the polling booth closes. Poll workers can then hand-deliver the cards to a designated place for tallying, or counties can set up secure, direct connections to move the data into a central repository. Companies are secretive about whether such transmissions would go over the Internet, but such a path seems likely in at least some cases.

Before the polls open, the machines provide a printout showing that there has been no voting

136

activity; at day's end, a similar printout shows total activity with tallies. If required, machines can also then print each of the ballots cast that day--though they cannot be traced to an individual.

E-voting advocates point to the many safeguards already built in against fraud and failure, including standardized federal certification of both software code and e-voting hardware by independent testing agencies (ITA). States often do their own review, too.

Pros and Cons

Moreover, they say, there are many benefits of e-voting. For example, computers aid disabled voters, by permiting them to magnify screen text or by reading the ballot aloud to them. Multilingual voters can see ballots in any of a dozen languages. Results can be tallied instantly. And military personnel and civilians overseas can vote online, confident that their ballots will count.

So where is the problem? According to Electronic Frontier Foundation activist Ren Bucholz, it comes down to three major things. The federal testing standards date back to 1990, and were only superficially updated in 2000. Government agencies plan further updates to these standards, but that has not happened yet.

Moreover, the ITA reports are not open to the public. The public got its initial view of e-voting code only when an activist downloaded 40,000 pages of documents from an unprotected Diebold Elections Systems FTP server in 2003. That security breach led to reports by Johns Hopkins and Rice University computer researchers about the system's alleged vulnerabilities, which Diebold has challenged.

Lastly, though printing capabilities exist, they're used after polls close. Given that, like any computer, an e-voting machine can fail or be hacked, critics demand an immediate, permanent record of each ballot, reviewable by a voter prior to ballot submission.

Controversy doesn't stop at the mechanics of the process. Diebold chief executive Walden O'Dell said in a letter to Ohio Republicans that he was committed to delivering the state's electoral votes to Bush in 2004 (he also contributed to Bush's campaign). Such remarks raise doubt about the impartiality of e-voting system makers, according to critics. O'Dell has since told The Plain Dealer, a Cleveland newspaper, that he regrets the wording of the letter and insists that he has no daily involvement with Diebold's election systems division, which he maintains is a model of integrity.

Remedies

Some change is already underway. Nevada law now requires that all e-voting machines in the state provide receipts for this year's election. Likewise, California has mandated that all e-votes in the state be confirmed with a paper receipt by 2006. Four other states have established the same requirement--but unlike California, they have not demanded that vendors retrofit existing systems to provide print-outs. Also, a few federal bills have been introduced (namely S.1980, S.1986, HR.2239) that mandate this requirement nationwide.

Kevin Shelley, California's secretary of state, has instituted stricter requirements for testing and auditing voting machine software as well.

The nation's three largest voting machine makers--ES&S, Diebold, and Sequoia Voting Systems--plan to offer paper-audit equipment; Sequoia's systems are ready now.

And e-voting companies are taking security concerns seriously. Six of them, along with the

Information Technology Association of America, formed the Election Technology Council. The ETC plans to write an ethical code for e-voting companies, and to review security procedures.

Even e-voting's most ardent critics acknowledge that election fraud is at least as old as the Republic. They are working not to block adoption, they say, but to ensure that e-voting systems are secure and reliable, and allow for independent recounts. The ETC and forthcoming paper receipts should help serve that goal.

Photograph by: Robert Cardin

Related Topics:

CBS .com

Electronic Voting Causing Concern

Jan. 3, 2003

As the curtain opens on this presidential election year, more Americans than ever will cast their votes electronically, **CBS News Correspondent Russ Mitchell** reports.

"Everybody who tried it thought it was terrific," said Margaret Luca, who supervises elections in Fairfax County, Virginia, where voters make their selections by simply touching a screen.

It turns out that not everybody thought it was terrific. Rita Thompson believes the machines cost her a second term on the County School Board, which she lost by just 1% of the vote.

Several people had started to complain about the fact that either they didn't see my name on the ballot, or it would take three or four times for the touch screen to light up my name," Thompson said.

Officials confirm that improper stacking of their machines may have damaged the touch screens in a way that cost Thompson votes on at least one machine, **Mitchell** reports. They can't be sure about all the other polling places because the machines, made by Advanced Voting Solutions, do not create a paper record of every vote.

"We have nothing to validate this election -- except they say, 'We believe the machines worked well,'" Thompson said.

States like Virginia had hoped the machines would help prevent the chad fiasco that made Florida a punch line, but there's a growing number of experts who question the accuracy and security of electronic voting.

Avi Rubin and a team of researchers examined software code developed by Diebold Election Systems, the largest manufacturer of electronic voting machines.

"There are many things that we teach in Security 101 that were not understood by the developers of these machines," Rubin said. "Within an hour of looking at the source code in the Diebold machines, we knew were looking at very bad code."

That code, Rubin says, was vulnerable to tampering that could manipulate vote totals. The researchers are especially critical of the so-called smart cards that control each machine - the card's PIN number was simply: 1-1-1-1.

"A 15-year-old in a garage could manufacture smart cards and sell them on the Internet that would allow for multiple votes," Rubin said.

Diebold Marketing Director Mark Radke says Rubin's team examined code that is not currently used in his company's machines. However, **Mitchell** reports, he admits that independent reviews by Ohio and Maryland have helped Diebold remedy potential weaknesses - like the PIN number.

"I wouldn't call them holes. I would say we enhanced the security of the system with some of the changes that were made," Radke said. "The touch screen machine and all electronic voting we offer is very secure."

Still, Diebold will not guarantee tamper-proof technology.

That's not good enough for California, which now requires their electronic machines to provide a ballot-by-ballot paper trail by 2006. Members of Congress are proposing similar legislation to expand such a requirement nationwide.

"That piece of paper would be kept by the voting machine and used in a recount," Rubin said.

But opponents argue that a record would require storing and securing thousands of pounds of paper.

"We are trying to get away from that kind of thing," Luca said.

The upcoming presidential primaries could make or break electronic voting's reputation, **Mitchell** reports. After the controversial election of 2000, voters may have little tolerance for being bitten by technical bugs.

"I'm afraid that they will sweep this under the rug and not look at the problem that happened in my instance, and not improve," Thompson said. "I don't want this to happen again."

Last week, a Washington-based software company that makes security software for electronic voting machines admitted that hackers broke into its computers and stole internal documents. The company, VoteHere, described the documents as "unsensitive."

©MMIV, CBS Broadcasting Inc. All Rights Reserved.

South Florida Sun-Sentinel

DEDICATED TO BEING THE MOST VALUED INFORMATION PROVIDER IN SOUTH FLORIDA

ROBERT GREMILLION
PUBLISHER

EARL MAUCKER
EDITOR

JOHN MCKEON
GENERAL MANAGER

SHARON ROSENHAUSE
MANAGING EDITOR

ESTABLISHED
NOV. 18, 1910

KINGSLEY GUY
EDITORIAL PAGE EDITOR

ELECTION REFORM

DON'T ADD PAPER BACKUP BALLOTS

County commissioners should heed some goo advice from a top county official: Don't rush to re quire voting machines to give voters a "backup" pa per ballot receipt. Instead, take a wait-and-see ap proach, because voting machine technology i evolving, paper ballots have many disadvantage and U.S. elections law may soon override county ac tions.

The advice comes from Pete Corwin, assistant t the county administrator, in a carefully researche 33-page memo. Commissioners sought his advice o possibly "retrofitting" each iVotronic touch-screen voting machine with a printer to provide an auditable "paper trail" produced by each voter.

Security procedures and controls, not printers, are the best way to ensure accuracy of any voting system.

He errs in saying that a voter-produced paper ballot could someday be a "desirable" option, but his other conclusions should be accepted:

■ While a "perfect" voting system doesn't exist, iVotronic machines and the system of programming and using them are "secure, reliable and accurate." With current security procedures and controls in place, the system can be relied on to do its job.

■ There is no printer in production to provide paper ballot receipts, and no printer certified by the state to do so. Printers probably could not be in place for the 2004 fall elections.

■ The introduction of printers and voter-printed ballots introduces major problems: Printers can jam and run out of paper and ink. Paper ballots mark an unwelcome return to human interpretation of "voter intent" and will take much longer to count. Voters may forget to put their printed ballots in the ballot box or argue that the ballot doesn't reflect how they intended to vote. Voting will take much longer than before. It may cost up to $6 million to add printers onto the 5,000 voting machines.

■ Don't switch to optically scanned voting machines. Operating costs are much higher, as are costs of printing hundreds of different ballot styles

and U.S. elections law may soon override county actions.

The advice comes from Pete Corwin, assistant to the county administrator, in a carefully researched 33-page memo. Commissioners sought his advice on possibly "retrofitting" each iVotronic touch-screen voting machine with a printer to provide an auditable "paper trail" produced by each voter.

Security procedures and controls, not printers, are the best way to ensure accuracy of any voting system.

He errs in saying that a voter-produced paper ballot could someday be a "desirable" option, but his other conclusions should be accepted:

■ While a "perfect" voting system doesn't exist, iVotronic machines and the system of programming and using them are "secure, reliable and accurate." With current security procedures and controls in place, the system can be relied on to do its job.

■ There is no printer in production to provide paper ballot receipts, and no printer certified by the state to do so. Printers probably could not be in place for the 2004 fall elections.

■ The introduction of printers and voter-printed ballots introduces major problems. Printers can jam and run out of paper and ink. Paper ballots mark an unwelcome return to human interpretation of "voter intent" and will take much longer to count. Voters may forget to put their printed ballots in the ballot box or argue that the ballot doesn't reflect how they intended to vote. Voting will take much longer than before. It may cost up to $6 million to add printers onto the 5,000 voting machines.

■ Don't switch to optically scanned voting machines. Operating costs are much higher, as are costs of printing hundreds of different ballot styles.

■ Security procedures and controls, not printers, are the best way to ensure accuracy of any voting system, and should be continually re-evaluated and strengthened. Broward should better track the "chain of custody" of who programs and sets up machines. Broward should upgrade to any "best practices" developed elsewhere for improved security.

With a new elections supervisor in place, the challenges of upgrading the elections office should take priority. Commissioners should not introduce any costly, controversial and complicated new challenges at this time by changing voting machines to add printers.

The New York Times

Technology

NEW ECONOMY

Considering Computer Voting

By JOHN SCHWARTZ
Published: December 15, 2003

Gaithersburg, Md.

HIGH-TECH voting is getting a low-tech backstop: paper. Most new voting machines are basically computers with touch screens instead of keyboards. Their makers promise that the new machines will simplify voting and forever end the prospect of pregnant and hanging chads. But as the market for computerized voting equipment has intensified, a band of critics has emerged, ranging from the analytical to the apoplectic.

Companies like
Systems make
that are basicall
touch screens.

The opponents of the current machines, along with the people who make them and election officials who buy them, gathered to spar in Gaithersburg, a Washington suburb, last Wednesday and Thursday, at a symposium optimistically titled, "Building Trust and Confidence in Voting Systems."

Advertisement

Am I providing the right IT services to support the needs of my business?

The critics complained that the companies were putting democracy into a mystery box, and that the computer code for the systems was not written to standards that ensure security. Critics are uneasy about the major vendors' political ties, and they worry about what a malevolent insider or a hacker could do to an election. But above all, they complain that few of the new machines allow voters to verify their votes, whether with a paper receipt or another method, an idea favored by computer scientists including David L. Dill of Stanford University.

The companies generally respond that the lever-style, mechanical voting machines offer no such backup, either. The critics counter that the computerized systems are the first to need voter verification methods.

ARTICLE TOC
E-Mail This
Printer-Frie
Most E-Mai
Reprints &
Single-Pag

TIMES NEWS
Topics
National Institut Standards and Technology
Politics and Go
Computers and Internet
Standards and Standardization
Create Your Ov
Most Popular A
CLICK HERE T

143

Now a growing number of election officials and politicians seem to be agreeing with the skeptics. Last week, Nevada said it was buying voting machines for the entire state, and it demanded paper receipts for all voters. Nevada Secretary of State Dean Heller said he received an overwhelming message from voters that they did not trust electronic voting. "Frankly, they think the process is working against them, rather than working for them," Mr. Heller, a Republican, said. Last month, the California secretary of state, Kevin Shelley said that his state would require all touch-screen voting machines to provide a "voter-verified paper audit trail."

Senator Hillary Rodham Clinton, Democrat of New York, has introduced a bill that would require a paper trail and security standards for voting machines. Her bill is similar to an earlier entry sponsored by a fellow Democrat, Representative Rush D. Holt of New Jersey. "What's required for money machines should be required for voting machines," Senator Clinton said in introducing the bill. "We must restore trust in our voting, and we must do it now."

Rebecca Mercuri, an expert on voting technology who is affiliated with Harvard's Kennedy School of Government and attended the symposium, said the tone of the discussion had changed from acrimony and accusation to the beginnings of civil conversation. The old corporate view, she said, was that "we have the safest, most secure voting machine - and by the way, it's a secret," Ms. Mercuri said. But that "is not going to provide the trust and confidence that we need," she said.

The symposium was at the National Institute of Standards and Technology. The institute, part of the Commerce Department, plans to develop programs to test and accredit voting systems under the Help America Vote Act, passed in 2002 after the bitterly contested 2000 elections. That law requires state and local officials to replace outdated voting systems, calls for minimum standards for the systems and provides federal funds to move the process along.

Companies that make electronic voting machines have scrambled to dominate the lucrative new market. They include Diebold Election Systems (a division of Diebold Inc.) Sequoia Voting Systems, Election Systems and Software, and Hart InterCivic.

The industry insists that its systems are secure and trustworthy, with or without paper. Harris Miller, who leads a new trade association for the industry, said that the group had no position in favor or against paper trails, but dismissed the issue as a "theological debate within the academic community." Mr. Miller, who is also president of the Information Technology Association of America, called some opponents of electronic voting "black helicopter theorists" and Luddites who "want to go back to the bad old days" of stuffed ballot boxes and chad wars.

NYT

Price: $195. L

nytimes.com
White Pap
Find credible r
you make infor
decisions.
Click here to d
White Paper

Get home delivery of The Times from $2.90/week

Continued
1 | 2 | Next>>

OUR ADVERT

Free IQ Test

Dell Axim hanc

144

ADVERTISER LINKS what's this?

Touch Panels / Screen
For touch panels and screens check out Fujitsu
us.fujitsu.com

Touch Screens
Manufacture specialty touch screens and monitors
cybertouch.com

Immersion Corporation
TouchSense™ Technology provides the Sense of Touch to the Digital World
www.immersion.com

affordable.

Learn about IB security.

TOP NYTIMES.COM ARTICLES

- U.S. Troops Beat Back Ambush in Central Iraq, Leaving 11 Dead
- Baker Has 'Fruitful' Talks With Chirac on Cutting Iraq's Debt
- President Signs Legislation Aiming to Stem Flood of Spam
- British Ignite Debate in U.S. on Drugs and Suicide

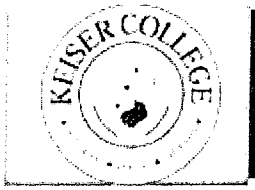
Go to NYTimes.com Home

TOP TECHNOLOGY ARTICLES

- EMC Acquires Software Maker for $635 Million
- Motorola Narrows to 2 Its Search for New Chief
- Accord Lets First Data Acquire Concord EFS
- Oracle Quarterly Earnings Beat Estimates by a Penny

Go to Technology

Copyright 2003 The New York Times Company | Home | Privacy Policy | Search | Corrections | Help | Back to Top



THE NEWS
Front Page
Local
Sports
Business
Publisher's Desk
Reader Services
Weather
Society
Features
Obituaries
Columns
Real Estate
Classifieds
Cartoons
Movies
OFF THE WIRE
Headlines
Business
Sports
Entertainment
SEARCH
go
This Site

Updated on January 7, 2004

This Afternoon: Partly cloudy with a high of 70

LOCAL NEWS

LePore opposes paper 'receipts' for voters

County elections chief says 'much misinformation'

Published Wednesday, January 7, 2004
by Dale M. King

Wherever embattled Palm Beach County Supervisor of Elections Theresa LePore goes, controversy seems to follow.
Right now, the woman who soared to notoriety on the wings of 2000's "butterfly ballot" debacle is explaining why voting "receipts" are not needed at the polls.
LePore told the Federation of Boca Raton Homeowner Associations Tuesday that voting equipment is tested again and again for accuracy. She said the county's touch-screen voting machines are "not computers, they are processors. They cannot be hooked up to a keyboard, they cannot be hacked into" and they are not networked to other voting machines.
She said data goes into three electronic collection "buckets" in the machine – and all the information must tally every time a vote is cast. If it doesn't, the voting apparatus shuts down.
Last month, U.S. Rep. Robert Wexler told an audience in Boca Raton last month that he has co-sponsored a bill requiring a paper trail to document all ballots punched into the county's new touch-screen ballot machines.
LePore said she wasn't invited to attend that meeting. "You don't invite your enemies," she said.
She said that session generated a lot of "misinformation."
"A paper receipt is not necessary because of the redundant memory" in the voting machines, she said. She said many civil liberties groups oppose paper balloting receipts – and a printer would be "another piece of equipment" that poll workers would have to learn to operate.
LePore said the task of hiring some 5,000 poll workers for Election Day is tough enough.
The cost of buying printers for 500 voting machines – at $600 to $1,000 each – is also prohibitive.
"If we are told to do it – and someone gives me the money – we will do it," she said.
In other matters, the election chief touched on several other

LATEST HEADLINES
SPORTS NEWS
FAU trounces Mary Washington, 101-61
LOCAL NEWS
Fleeing France
LOCAL NEWS
Autopsy confirms homicide
LOCAL NEWS
DNA database nabs Delray Beach man suspected in 2000 rape case
LOCAL NEWS
Boca soldier heading to Iraq
SURVEY

cont@ct us

topics.

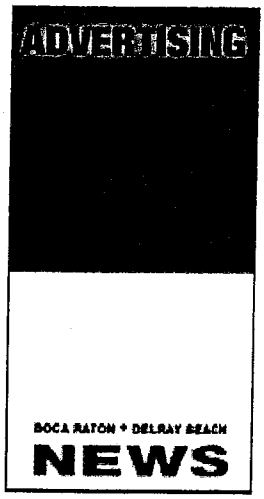
• LePore said she has adjusted polling places in Boca Raton to reflect the annexation of Town Center at Boca Raton mall and several other business and residential areas. As a result of annexations in Boca and other areas, she has added more than 40 new precincts, bringing the number in the county to 680.

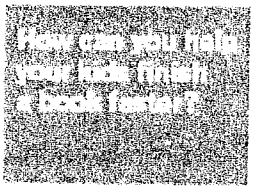
• She also said she is running for re-election this year. The sheriff, supervisor of elections and property appraiser are now non-partisan races. She said two people have announced they may run against her. If both file, LePore would face a primary challenge Aug. 31. If she is unopposed or has only one foe, she will run Nov. 2.

• The presidential preference primary in Florida will be held March 9. That is the same day as municipal elections in Boca Raton and Delray Beach.

Send this page to a friend

Copyright 2003 - Boca Raton News



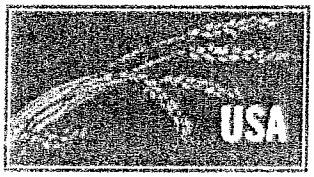


Audio update: The hour's top news headlines live in RealAudio from AP Radio.

The Leader in Local News
Boca Raton News

©1998-2002 The Boca Raton News

POWERED BY
Accri



DOMESTIC POLITICS
ECONOMY
FOREIGN POLICY
JUSTICE
MILITARY
SOCIETY & CULTURE

Also see:
Iraq in Transition
Living > Religion & Ethics

Monitor Breakfast
Bacon, eggs, and policy: Fill your plate with excerpts from discussions between reporters and Washington newsmakers.

USA Stories:
for 11/03/2003

The case for war under new focus

Kentucky as bellwether for Bush's job policies

For mutual-fund clients, a question of confidence

Drugs in the car, and no one owns up. Is everyone liable?

Iowa caucus: the way of the dinosaur?

Tales of heroism and narrow escape after an epic week on the front lines

A better ballot?

USA > Domestic Politics
from the November 03, 2003 edition

A better ballot?

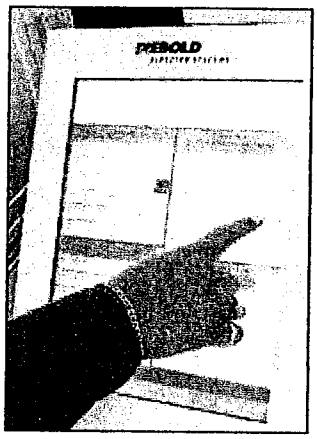
Electronic ballots, hailed as the antidote to hanging chads, will make a mark on Election Day. But critics warn of risks to democracy.

By Mary Wiltenburg | *Staff writer of The Christian Science Monitor*

When voters head to the polls Tuesday, those using punch-card ballots - notorious for their role in the 2000 presidential election recount - may do so with a lingering unease that their votes could go uncounted. Others will enter sleek new electronic voting booths bought at great price by a patchwork of states and counties trying to guard against butterfly ballots and hanging chads.

But a growing number of computer scientists are now warning that the new technology, far from solving America's voting problems, may actually make things worse. Electronic ballots can be miscounted too, they say - or the machines that tally them tampered with and traces of sabotage erased.

"If you look at the consequences for democracy, it's terrifying," says David Dill, a Stanford University computer-science professor who has led the charge to raise awareness about the machines' potential security flaws. "If we had a way to make [computerized voting] safe, believe me, we would. There's no way to run a reliable election without a verifiable paper trail - that's what these machines don't have."



NEW METHOD: One in 10 voters used electronic touch-screen ballots during California's Oct. 7 recall election.

Others, including makers of the electronic systems and politicians who tout them, argue that democracy always has been a messy process and that no technology is foolproof. As long as

SUPPORT
→ Make a

MONITO

Purchase
the Monito
as little as

TREELE
New! Su
Treele

SUB
Subscribe
Free sa
E-mail He

XML What is this?

SPECIAL PROJECTS

Empire Builders

September 11 One year later

Defining Terrorism

Amtrak: All Aboard?

My Fellow Americans...

The Heart of a High School

more projects...

Most-viewed stories:
(for 11/02/03)

11/03/03
The case for war under new focus

11/03/03
Kentucky as bellwether for Bush's job policies

11/03/03
A deadly day and a US strategy shift

10/31/03
Things that go 'yuck!' in the night

10/31/03
Solar flare reveals physics of an angry sun

there's been a vote, they say, there have been ballots destroyed, misread, and counterfeited; machines worn out or sabotaged; officials bribed; voters bullied or denied their rights. Some disabled citizens have been unable to vote privately, illiterates have been unable to vote knowingly, and voters with limited English have not understood how to cast ballots that count. Electronic voting is the latest in a long line of imperfect solutions, its proponents say, but it's the best option there is.

Voting was a matter of assessing shouts and shows of hands back in Colonial days. In the 1770s, these unverifiable counts were replaced by ballots written longhand, which left a paper trail but took a long time to tally. In 1892, self-tallying lever machines sped up the process, but again left no paper record. When punch-card ballots hit the scene in the 1960s, jurisdictions began to replace the old lever machines. But the punch-card system had its own weaknesses. Even before the 2000 Florida fiasco, some states had switched to the mark-sense or optical-scan ballots, which are much like fill-in-the-bubble standardized tests.

After the recount debacle, officials scrambled to ensure that no future chads would be left hanging. Congress passed the Help America Vote Act of 2002 (HAVA), but has so far supplied only $664.5 million to fund it. So solutions have come in fits and starts, with counties adopting a hodgepodge of systems (see map). Last November, Georgia became the first state to install touch-screen machines at all its polling stations, under a $54 million contract with Diebold Election Systems, a supplier of Direct Recording Electronic voting systems (DREs).

Many Georgia voters were impressed. Kim Hullett, who used a new model in Fayette County's latest election, says the machines - which work much like automatic teller machines - were easy to understand, kept lines moving, and meant she and her husband could track election results on the Web as they heard about them on the TV news.

But Professor Dill, at Stanford, had doubts. A concerned activist had sent him a copy of the Diebold system's source code - the road map to its computer voting software - which the company had been storing on a publicly accessible server. Diebold says this code was partial and outdated. Dill gave the code to a team of computer security experts led by Avi Rubin, technical director of the Information Security Institute at Johns Hopkins University.

The team's report, released in July, marked the first time any company's voting-system software has been publicly evaluated by an academic team. Over 24 pages, it details what Dr. Rubin describes as system-security flaws the average teenager today would be

JIM RUYMEN/REUTERS

Related stories:

10/30/02
Voting technology: Will the chads still hang?

monitortalk

Weigh in on issues of the day in our forums.

E-mail this story

Write a letter to the Editor

Printer-friendly version

Permission to reprint/republish

Enter your receive ne

SCHOOL
Program
and

Th
Re
America

200
Com
Buy
Phot

computer-savvy enough to exploit.

Two big flaws, Rubin says, could give rise to any number of nightmare scenarios. The first: The machines' software is encrypted in only the most basic ways, so people with access to a machine before Election Day could easily get into it and, for instance, change the program so that all votes for one candidate go to an opponent. The second: Diebold machines, like comparable machines sold by Sequoia Voting Systems and Election Systems & Software, produce no paper record of a vote, making recounts impossible. A computer science professor, Rubin says he's all in favor of computerizing needless paperwork - but sometimes, in the interest of democracy, you need to kill a few trees.

Diebold rebutted the team's report, arguing it failed to take into account all the checks and balances that ensure election security. Rubin's team argued back that poll workers cannot be expected to make up for security flaws in election machines.

Caught in the crossfire, Maryland put on hold a $55.6 million contract with Diebold to outfit the entire state, and asked Scientific Applications International Corp., an independent research firm, to investigate. Though the firm's report cautiously confirmed some of the Rubin team's findings, it said many flaws could be corrected, and Maryland decided to go ahead with the purchase. Last month, two lawmakers requested a further review of the matter by an independent state agency.

Meanwhile, states are in limbo - awaiting word on the security of DRE machines before spending more on them, as well as late-arriving HAVA funding. The 2002 act mandates numerous state and county reforms, such as establishing reliable voter rolls (many African-Americans were mistakenly cut from Florida's 2000 eligible-voter lists, and in Denver last month, nearly 200 deceased voters were invited to cast absentee ballots).

The law does not require states to install electronic systems, but the technology holds appeal because of its flexibility, says Roy Saltman, a private election- technology consultant. DREs can give instructions in many languages, and can be adapted for visually impaired voters. HAVA requires that all new systems and safeguards be in place by January 2006, a deadline many states expect to miss.

Critics and some proponents of DREs agree on one thing: the need for a paper audit trail so votes can be recounted. A bill now before Congress would add that requirement.

From quill to touch screen: a US history of ballot-casting

1770s Balloting replaces a show of hands or voice votes. Voters write out names of their candidates in longhand, and give their ballots to an election judge.

1850s Political parties disperse preprinted lists of candidates,

enabling the illiterate to vote. The ballot becomes a long strip of paper, like a railroad ticket.

1869 Thomas Edison receives a patent for his invention of the voting machine, intended for counting congressional votes.

1888 Massachusetts prints a ballot, at public expense, listing names of all candidates nominated and their party affiliation. Most states adopt this landmark improvement within eight years.

1892 A lever-operated voting machine is first used at a Lockport, N.Y., town meeting. Similar machines are still in use today.

1964 A punch-card ballot is introduced in two counties in Georgia. Almost 4 in 10 voters used punch cards in the 1996 presidential election.

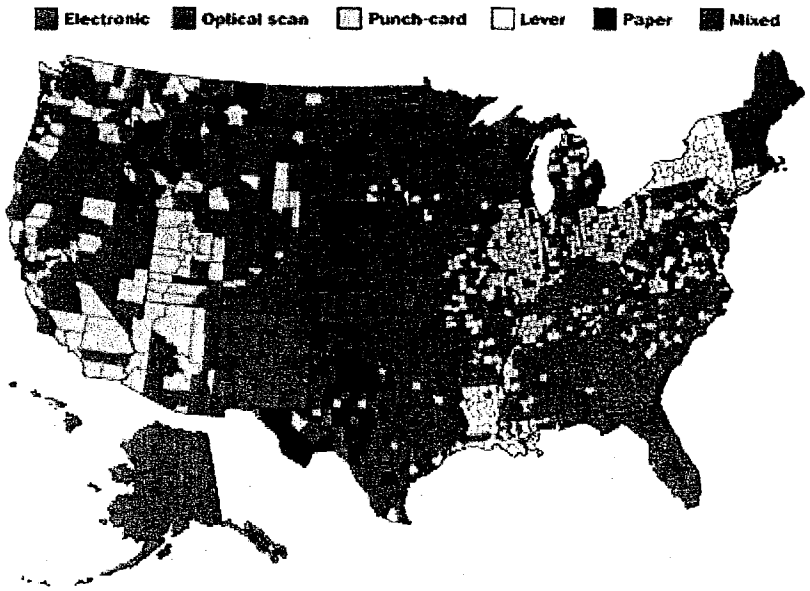
1990s Michigan is the first to switch to optical scanning, used for decades in standardized testing. One-quarter of voters used the technology in the 1996 election.

2000 A storm erupts over Florida's punch-card ballots and Palm Beach County's "butterfly ballot" in the presidential election.

2002 New federal law authorizes $3.9 billion over three years to help states upgrade voting technologies and phase out punch cards and lever machines. Georgia is the first state to use DRE touch-screen technology exclusively.

Sources: Federal Elections Commission; "Elections A to Z," CQ, 2003; International Encyclopedia of Elections, CQ Press, 2000; League of Women Voters

HOW A NATION VOTES: In response to the 2000 presidential recount fiasco, Congress has required states to replace outmoded lever and punch-card voting machines by the 2006 election. Meantime, a county-by-county look at how the American electorate will cast its votes Tuesday.



Order Code RL32139

CRS Report for Congress
Received through the CRS Web

Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues

November 4, 2003

Eric A. Fischer
Senior Specialist in Science and Technology
Domestic Social Policy Division

152

Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues

Summary

In July 2003, computer scientists from Johns Hopkins and Rice Universities released a security analysis of software purportedly from a direct recording electronic (DRE) touchscreen voting machine of a major voting-system vendor. The study drew public attention to a long-simmering controversy about whether current DREs are vulnerable to tampering that could influence the outcome of an election.

Many innovations that have become familiar features of modern elections, such as the secret ballot and mechanical lever voting machines, originated at least in part as a way to reduce election fraud and abuse. Computer-assisted counting of ballots, first used in the 1960s, can be done very rapidly and makes some kinds of tampering more difficult. However, it does not eliminate the potential for fraud, and it has created new possibilities for tampering through manipulation of the counting software and hardware. DREs, introduced in the 1970s, are the first voting systems to be completely computerized. Touchscreen DREs are arguably the most versatile and user-friendly of any current voting system. Their use is expected to increase substantially under provisions of The Help America Vote Act of 2002 (HAVA, P.L. 107-252), especially the requirement that, beginning in 2006, each polling place used in a federal election have at least one voting machine that is fully accessible for persons with disabilities.

With DREs, unlike document-ballot systems, the voter sees only a representation of the ballot; votes are registered electronically. Some computer security experts believe that this and other features of DREs make them more vulnerable to tampering than other kinds of voting systems, especially through the use of malicious computer code. While there are some differences of opinion among experts about the extent and seriousness of those security concerns, there appears to be an emerging consensus that in general, current DREs do not adhere sufficiently to currently accepted security principles for computer systems, especially given the central importance of voting systems to the functioning of democratic government. Others caution, however, that there are no demonstrated cases of computer tampering in public elections, and any major changes that might be made to improve security could have unanticipated negative effects of their own. Several proposals have been made to improve the security of DREs and other computer-assisted voting systems. They include (1) ensuring that accepted security protocols are followed appropriately, (2) improving security standards and certification of voting systems, (3) use of open-source computer code, and (4) improvements in verifiability and transparency.

Much of the current debate has focused on which such proposals should be implemented and through what means — in particular, whether federal involvement is necessary. Some states are already addressing these issues. The Election Assistance Commission established by HAVA will have some responsibilities relating to voting system security and could address this controversy directly. Some observers have also proposed federal funding for research and development in this area, while others have proposed legislative solutions including enhancement of the audit requirements under HAVA.

Contents

Background and History of the Issue 2
- Australian Secret Ballot 2
- Mechanical Lever Machine 3
- Computer-Assisted Counting (Punchcard and Optical Scan) 3
- Electronic Voting Machine 3
- DREs and HAVA 4
- Security Concerns about DREs 5

Analysis of the Problem 10
- Threats 10
  - Kinds of Attacks and Attackers 10
  - An Evolving Threat Environment 11
- Vulnerabilities 12
  - Technical Vulnerabilities 12
  - Social Vulnerabilities 15
- Defense 16
  - Goals of Defense 16
  - Elements of Defense 18
  - Trade-Offs 19
- Response and Recovery 20
- Confidence in DREs 21

Proposals for Resolving the Issue 22
- Use Current Procedures 22
- Improve Security Standards and Certification of Voting Systems 23
- Use Open Source Software 26
- Improve Verifiability and Transparency 27
  - Voter-Verifiable Paper Ballot 28
  - Votemeter 29
  - Modular Voting Architecture 29
  - Encrypted Votes 30

Options That Might Be Considered 32
- States 33
- EAC 33
- Congress 33

Conclusions 35

Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues

In July 2003, computer scientists from Johns Hopkins and Rice Universities released a security analysis of software purportedly from an electronic voting machine (commonly called direct recording electronic, or DRE, systems) of a major voting-system vendor.[1] The Hopkins study drew public attention to a long-simmering controversy about whether current DREs are vulnerable to tampering that could influence the outcome of an election. A significant factor contributing to this increased attention is the Help America Vote Act of 2002 (HAVA, P.L. 107-252), which substantially increases the federal role in election administration, including federal funding of and requirements for voting systems. Although HAVA retains the predominant role that state and local jurisdictions have traditionally had in the administration of elections, the Act's requirements are expected to result in increased use of DREs, and some observers have therefore called for congressional action to address the DRE controversy. To understand this controversy requires an examination of several questions about voting-system security:

- Do DREs exhibit genuine security vulnerabilities? If so, could those vulnerabilities be exploited to influence an election?
- To what extent do current election administration procedures and other security measures protect against threats to and vulnerabilities of DRE systems?
- Do those threats and vulnerabilities apply to computer-assisted voting systems other than DREs?
- What are the options for addressing any threats and vulnerabilities that do exist, and what are the relative strengths and weaknesses of the different options?

To address those questions, this report begins with a description of the historical and policy context of the controversy. That is followed by an analysis of the issues in the broader context of computer security. The next section discusses several proposals that have been made for addressing those issues, and the last section discusses options for action that might be considered by policymakers. The report

---

[1] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, "Analysis of an Electronic Voting System," *Johns Hopkins Information Security Institute Technical Report TR-2003-19,* July 23, 2003, [http://avirubin.com/vote/] (called the Hopkins study hereinafter).

does not discuss Internet voting, which is not likely to be used in the near future for federal elections in other than minor ways, largely because of security concerns.[2]

The administration of elections is a complex task, and there are many factors involved in choosing and using a voting system in addition to security. They include factors such as reliability, propensity for voter error, usability, and cost. This report does not discuss those factors, but election administrators must consider them in decisions about what systems to use and how to implement them. Also, security is an issue for other aspects of election administration, such as voter registration, which are beyond the scope of this report.

Background and History of the Issue

Many innovations that have become familiar features of modern elections originated at least in part as a way to reduce election fraud such as tampering with ballots to change the vote count for a candidate or party. For example, in much of nineteenth century America, a voter typically would pick up a paper ballot preprinted with the names of candidates for one party and simply drop the form into the ballot box. There was no need to actively choose individual candidates.[3] This ticket or prox ballot was subject to fraud in at least two ways. First, the number and sequence of ballots printed was not controlled, so it could be difficult to determine if a ballot box had been stuffed with extra ballots or if ballots had been substituted after votes were cast. Second, an observer could determine which party a voter had chosen by watching what ballot the voter picked up and deposited in the ballot box — votes could therefore be bought or coerced with comparative ease.

Australian Secret Ballot. After a series of scandals involving vote-buying in the 1880s, calls for reform led to widespread adoption of the Australian or mark-choice ballot.[4] Such ballots list the names of all candidates, and the voter marks the ballot to choose among them. The ballots are commonly printed with unique, consecutive serial numbers, facilitating ballot control and thereby helping to prevent ballot stuffing and substitution. All printed ballots are otherwise identical, and voters typically fill them out in the privacy of a voting booth. This ballot secrecy makes it difficult for anyone else to know with certainty what choices a voter has made. While providing improved security, the Australian secret ballot did not eliminate

---

[2] In 2000, Internet voting was offered in pilot projects during primaries in Arizona and Alaska. A small pilot program for military and overseas voters was run for the general election by the Federal Voting Assistance Project (FVAP) under the Department of Defense. FVAP is expected to repeat the effort for the 2004 federal election. While the program used the Internet to transmit ballots to local jurisdictions in a secure fashion, the ballots were then printed and counted in the same way as other absentee ballots. See Kevin Coleman, *Internet Voting,* CRS Report RS20639, 23 September 2003.

[3] To choose a different candidate than the one printed on the ballot required crossing out the candidate's name and writing in another. Some party operatives developed ballots that made it difficult to perform write-ins — for example, by printing the names in very small type and cramming them together on a narrow strip of paper (See Richard Reinhardt, "Tapeworm Tickets and Shoulder Strikers," *American West* 3 (1966): 34-41, 85-88).

[4] S.J. Ackerman, "The Vote that Failed," Smithsonian Magazine, November 1998, 36,38.

tampering. Ballots could still be removed, spoiled, or altered by corrupt pollworkers, or even substituted or stuffed, although with greater difficulty than with prox ballots. It also did not eliminate the possibility of vote-buying or coercion, but it made them more difficult.[5]

Mechanical Lever Machine. One way to eliminate some means of ballot tampering is to eliminate document ballots. That became possible with the introduction of the lever voting machine in 1892. With this system, a voter enters the voting booth and sees a posted ballot with a small lever near the name of each candidate or other ballot choice. The voter chooses a candidate by moving the appropriate lever. Mechanical interlocks prevent voters from choosing more candidates than permitted for an office (such as two candidates for President). After completing all choices, the voter pulls a large lever to cast the ballot, and the votes are recorded by advances in mechanical counters in the machine. The lever machine therefore eliminates the need to count ballots manually. Instead, pollworkers read the numbers recorded by the counters. Because there is no document ballot, recounts and audits are limited to review of totals recorded by each machine. Of course, tampering is also possible with lever machines. For example, the mechanisms could be adjusted so that the counter does not always advance when a particular candidate is chosen.

Computer-Assisted Counting (Punchcard and Optical Scan). Another major technological advance in voting — the first use of computers to count votes — came with the introduction of the punchcard system, first used in 1964. The optical-scan voting system, which also uses computers for vote-counting, was first used in the 1980s. In both kinds of voting system, document ballots are fed into an electronic reader and the tallies stored in computer memory and media. Tallying can be done at either the precinct or a central location. Computer-assisted counting of document ballots can be done very rapidly, thus speeding the reporting of election results. It is much more efficient for counting large numbers of ballots than manual tallying. It makes some kinds of tampering more difficult than with manual counting, but it does not eliminate them, and it creates possibilities for tampering with the counting software and hardware.

Electronic Voting Machine. DREs (direct recording electronic systems) are the first completely computerized voting systems. They were introduced in the 1970s. DREs are somewhat analogous to (although more sophisticated than) lever machines. The voter chooses candidates from a posted ballot. Depending on the equipment used, the ballot may be printed and posted on the DRE, as it is with a lever machine, or it may be displayed on a computer screen. Voters make their choices by pushing buttons, touching the screen, or using other devices. The voter

---

[5] Some observers have expressed concern that use of absentee ballots and other kinds of remote voting, such as via the Internet, compromise ballot secrecy and therefore increase the risk of vote buying and coercion. They are concerned about the impacts that the growing use of absentee voting in the United States might have on election fraud and abuse. Others, in contrast, believe that the risks are small and greatly outweighed by the benefits. For a general discussion of the benefits and disadvantages of different kinds of voting systems, see Eric Fischer, *Voting Technologies in the United States: Overview and Issues for Congress,* CRS Report RL30773, 21 March 2001.

submits the choices made before leaving the booth, for example by pushing a "vote" button, and the votes are then recorded electronically.

There is considerable variability in the design of DREs, but they can be classified into three basic types. The oldest design essentially mimics the interface of a lever machine. The entire posted ballot is visible at once. Instead of moving levers to make choices, the voter pushes a button next to a candidate's name, or pushes on the name itself, triggering an underlying electronic microswitch and turning on a small light next to the choice. With the second type, a ballot page is displayed on a computer screen, and the voter uses mechanical devices such as arrow keys and buttons to make choices on a page and to change ballot pages. The third type is similar to the second except that it has a touchscreen display, where the voter makes a choice by touching the name of the candidate on the computer screen and casts the ballot by pressing a separate button after all choices have been made. In all kinds of DREs, when a ballot is cast, the votes are directly stored in a computer memory device such as a removable memory card or nonvolatile memory circuit. As with lever machines, there is no document ballot, although with a DRE each cast ballot may also be separately recorded.

Touchscreen and other DREs using computer-style displays are arguably the most versatile and user-friendly of any current voting system. Each machine can easily be programmed to display ballots in different languages and for different offices, depending on voters' needs. It can also be programmed to display a voter's ballot choices on a single page for review before casting the vote. It can be made fully accessible for persons with disabilities, including visual impairment.[6] Like lever machines, it can prevent overvotes and ambiguous choices or spoilage of the ballot from extraneous marks, since there is no document ballot; but it can also notify voters of undervotes.[7] No other kind of voting system possesses all of these features.

DREs and HAVA. The popularity of DREs, particularly the touchscreen variety, has grown in recent years,[8] and their use is expected to increase substantially under provisions of HAVA. Three provisions in the Act are likely to provide such an impetus. First, HAVA authorized $3.65 billion over four years for replacing punchcard and lever machines and for making other election administration improvements, including meeting the requirements of the Act. In FY2003, Congress appropriated $1.48 billion for these purposes (P.L. 108-7), and the Administration requested $500 million for FY2004. Second, beginning in 2006, HAVA requires that voting systems notify voters of overvotes and permit them to review their ballots and

---

[6] Accessibility for blind persons usually involves use of an audio program.

[7] An *overvote* occurs if a voter chooses more candidates for an office than is permitted — such as marking two candidates for President of the United States. An *undervote* occurs if a voter chooses fewer candidates than is permitted — most commonly, failing to vote for any candidate for a particular office. Virtually all overvotes are thought to be errors, whereas undervotes are often thought to be intentional, for example if the voter does not prefer any of the candidates. However, undervotes can also result from voter error.

[8] In 1980, about 1 out of every 40 voters used DREs. By 2000, about 1 out of every 9 did (Caltech/MIT Voting Technology Project, *Voting: What Is, What Could Be,* July 2001, [http://www.vote.caltech.edu/Reports/index.html] (Caltech/MIT study)).

correct errors before casting their votes.[9] Third, the Act requires, also beginning in 2006, that each polling place used in a federal election have at least one voting machine that is fully accessible for persons with disabilities. DREs are the only machines at present that can fulfill the accessibility requirement. They can also easily meet the requirements for error prevention and correction.

Security Concerns about DREs. One thing that distinguishes DREs from document ballot systems is that with DREs, the voter does not see the actual ballot, but rather a representation of it on the face of the machine. With few exceptions, current DREs do not provide a truly independent record of each individual ballot that can be used in a recount to check for machine error or tampering. The ballot itself consists of redundant electronic records in the machine's computer memory banks, which the voter cannot see. This is analogous to the situation with mechanical lever voting machines, where casting the ballot moves counters that are out of view of the voter. In a lever machine, if the appropriate counters do not move correctly when a voter casts the ballot, the voter will not know, nor would an observer. Similarly, with a DRE, if the machine recorded a result in its memory that was different from what the voter chose, neither the voter nor an observer would know.[10]

The same is true with a computerized counting system when it reads punchcards or optical scan ballots. Even if the ballot is tabulated in the precinct and fed into the reading device in the presence of the voter, neither the voter nor the pollworker manning the reader can see what it is recording in its memory. However, with such a reader, the ballot documents could be counted on another machine or by hand if there were any question about the results.

Lever machines also do not have an independent document ballot. That has led some observers to distrust those machines, but most who use them appear confident that tests and other procedural safeguards render them sufficiently safe from tampering. Is the same true for DREs? Some computer experts think not, arguing that the software could be modified in ways that could alter the results of an election and that would be very difficult to detect. This concern appears to stem largely from three factors:

- Malicious computer code, or *malware,* can often be written in such a way that it is very difficult to detect.[11]

---

[9] However, jurisdictions using hand-counted paper ballots, punchcards, or central-count systems can rely instead on voter education and instruction programs.

[10] Some kinds of error could be detected when voter registers and vote tallies are reconciled — for example, if the total number of votes for an office were greater than the total number of voters at the precinct. However, resolving such a problem in a way that reflects how voters actually voted would not be straightforward.

[11] *Malware,* an elision of *malicious software,* includes viruses, Trojan horses, worms, logic bombs, and any other computer code that has or is intended to have harmful effects. There are various ways of hiding malware. A Trojan horse, for example, is malware disguised as something benign or useful. See Kenneth Thompson, "Reflections on Trusting Trust," *Communications of the ACM* 27 (1984): 761-763, available at

(continued...)

- DRE software is moderately complex, and it is generally accepted that the more complex a piece of software is, the more difficult it can be to detect unauthorized modifications.[12]
- Most manufacturers of DREs treat their software code as proprietary information and therefore not available for public scrutiny. Consequently, it is not possible for experts not associated with the companies to determine how vulnerable the code is to tampering.[13]

Voting System Standards and Certification. Concerns such as those described above have been voiced by some experts at least since the 1980s.[14] The development of the Voluntary Voting Systems Standards (VSS) by the Federal Election Commission (FEC) in 1990, and the subsequent adoption of those standards by many states, helped to reduce those concerns. The VSS were developed specifically for computer-assisted punchcard, optical scan, and DRE voting systems. They include a chapter on security, which was substantially expanded in the updated version, released in 2002.[15] Along with the standards, a voluntary testing and certification program was developed and administered through the National Association of State Election Directors (NASED). In this program, an independent test authority (ITA) chosen by NASED tests voting systems and certifies those that comply with the VSS.[16] Testing is done of both hardware and software, and the tested software and related documentation is kept in escrow by the ITA.[17] If

---

[11] (...continued)
[http://www.acm.org/classics/sep95]. He concluded that it can be essentially impossible to determine whether a piece of software is trustworthy by examining its source code, no matter how carefully. The entire system must be evaluated, and even then it can be very difficult to find malware. However, use of modern software engineering techniques can minimize many problems with software design that can make software vulnerable to malware (see, for example, Richard C. Linger and Carmen J. Trammell, "Cleanroom Software Engineering Reference Model, Version 1.0," Technical Report CMU/SEI-96-TR-022, November 1996, available at [http://www.sei.cmu.edu/pub/documents/96.reports/pdf/tr022.96.pdf]). See page 12–14 of this report for further discussion of this issue.

[12] See page 13 for further discussion of this issue.

[13] See page 26 for further discussion of this issue.

[14] See, for example, Ronnie Dugger, "Annals of Democracy (Voting by Computer)," *The New Yorker,* 7 November 1988, 40-108; Roy G. Saltman, "Accuracy, Integrity, and Security in Computerized Vote-Tallying," *NBS Special Publication 500-158,* August 1988.

[15] See Federal Election Commission, *Voting Systems Performance and Test Standards,* 30 April 2002, [http://www.fec.gov/pages/vssfinal/vss.html].

[16] See NASED, "General Overview for Getting a Voting System Qualified", 30 September 2003, [http://www.nased.org/ITA_process.htm]. The program is managed by The Election Center, [http://www.electioncenter.org]. As of September 2003, more than 20 optical scan and DRE voting systems were listed as certified through this process.

[17] It may also be kept by the states (The Election Center, "DREs and the Election Process," April 2003, [http://www.electioncenter.org/newstuff/DREs%20and%20the%20Election
(continued...)

questions arise about whether the software used in an election has been tampered with, that code can be compared to the escrowed version. Systems that receive NASED certification may also need to go through state and local certification processes before being used by an election jurisdiction.

HAVA creates a new mechanism for the development of voluntary voting system standards. It creates the Election Assistance Commission (EAC) to replace the FEC's Office of Election Administration and establishes three bodies under the EAC: a 110-member Standards Board consisting of state and local election officials, a 37-member Board of Advisors representing relevant government agencies and associations and fields of science and technology, and a 15-member Technical Guidelines Development Committee chaired by the Director of National Institute of Standards and Technology (NIST). This last committee is charged with making recommendations for voluntary standards (called guidelines in the Act), to be reviewed by the two boards and the EAC.[18]

HAVA also requires the EAC to provide for testing, certification, and decertification of voting systems and for NIST to be involved in the selection and monitoring of testing laboratories. The EAC is also required to perform a study of issues and challenges — including the potential for fraud — associated with electronic voting, and periodic studies to promote accurate, secure, and expeditious voting and tabulation. HAVA also provides grants for research and development on security and other aspects of voting systems. The voting system requirements in the Act do not specifically mention security but do require that each voting system produce a permanent paper audit document for use as the official record for any recount. This requirement is for the system, not for each ballot. For example, most DREs can print a tally of votes recorded and therefore can meet this requirement.

The Caltech/MIT Study. The problems identified after the November 2000 federal election prompted wide public concern about voting systems and led to several major studies[19] with recommendations, many of which were incorporated in

---

[17] (...continued)
%20Process%204-2003.doc]).

[18] HAVA does not direct the EAC to include any specific issues in the guidelines, although the guidance must address the specific voting system requirements in the Act, and NIST is directed to provide technical support with respect to security, protection and prevention of fraud, and other matters. However, in the debate on the House floor before passage of the conference agreement on October 10, 2002, a colloquy (*Congressional Record,* daily ed., 148: H7842) stipulated an interpretation that the guidelines specifically address the usability, accuracy, security, accessibility, and integrity of voting systems.

[19] Studies that specifically addressed the security of voting systems included the Caltech/MIT study; The Constitution Project, Forum on Election Reform, *Building Consensus on Election Reform,* August 2001, [http://www.constitutionproject.org/eri/CPReport.pdf]; The National Commission on Federal Election Reform, *To Assure Pride and Confidence in the Electoral Process,* August 2001, [http://www.reformelections.org/data/reports/99_full_report.php]; National Conference of State Legislatures, Elections Reform Task Force, *Voting in America,* August 2001, [http://www.ncsl.org/programs/press/2001/
(continued...)

HAVA. The most extensive examination of security was performed by scientists at the California Institute of Technology and the Massachusetts Institute of Technology. Their report identified four main security strengths of the electoral process that has evolved in the United States: the openness of the election process, which permits observation of counting and other aspects of election procedure; the decentralization of elections and the division of labor among different levels of government and different groups of people; equipment that produces "redundant trusted recordings" of votes; and the public nature and control of the election process.[20] The report expressed concern that current trends in electronic voting are weakening those strengths and pose significant risks, but that properly designed and implemented electronic voting machines can improve, rather than diminish, security.

The California Task Force Report. The concerns expressed by the Caltech/MIT study and others were partially addressed by HAVA, but as states began to acquire DREs, and the appointment of EAC members was delayed,[21] some observers began expressing concerns that states were purchasing flawed machines with no federal mechanism in place for addressing the problems. In response to such concerns, the California secretary of state established a task force to examine the security of DREs and to consider improvements. The report[22] recommended changes to how voting systems are tested at the federal, state, and local levels, as well as other changes in security for software and for vendor practices. It also recommended the implementation of a voter-verified audit trail — that is, a mechanism, whether paper-based or electronic, that produces an independent record of a voter's choices that the voter can verify before casting the ballot and that can be used as a check against tampering or machine error. Until such a system can be implemented, the task force recommended the use of "parallel monitoring," in which a selection of machines are tested while in actual use on election day to determine if they are recording votes accurately.

The Hopkins Study. Until recently, the concerns raised about DRE vulnerabilities were considered by many to be largely hypothetical. However, in early 2003, some election-reform activists discovered[23] an open website containing

---

[19] (...continued)
electref0801.htm].

[20] Some international observers consider openness and public control to be important components of any voting system (Lilian Mitrou and others, "Electronic Voting: Constitutional and Legal Requirements, and Their Technical Implications," in *Secure Electronic Voting,* ed. Dimitris Gritzalis (Boston: Kluwer, 2003), p. 43-60).

[21] HAVA calls for appointment of members by February 26, 2003. On October 3, 2003, the White House forwarded nominations to the Senate for confirmation. The nominations were referred to the Committee on Rules and Administration, which held a hearing on the nominations on October 28.

[22] California Secretary of State Kevin Shelley, "Ad Hoc Touch Screen Task Force Report," 1 July 2003, [http://www.ss.ca.gov/elections/taskforce_report.htm] (California Task Force report).

[23] Bev Harris, "System Integrity Flaw Discovered at Diebold Election Systems," *Scoop,* 10
(continued...)

large numbers of files relating to voting systems of Diebold Election Systems, a major voting system vendor which had recently won contracts with Georgia and Maryland to provide touchscreen DREs. Activists downloaded and posted many of those files on Internet sites, and the authors of the Hopkins study used some of those files to analyze computer source code that "appear[ed] to correspond to a version of Diebold's voting system."[24] Their analysis concluded that the code had serious security flaws that could permit tampering by persons at various levels, including voters, election workers, Internet "hackers," and even software developers. Diebold quickly rebutted those claims,[25] arguing that they were based on misunderstanding of election procedures and of the equipment within which the software was used, and that the analysis was based on an "inadequate, incomplete sample" of Diebold's software. Some computer scientists, while agreeing that the code contained security flaws, also criticized the study for not reflecting standard election procedures.[26]

Shortly after the Hopkins study was released, Maryland Governor Robert Ehrlich ordered that the contract with Diebold be suspended pending the outcome of an independent security analysis. That analysis,[27] while agreeing with several of the criticisms of the Hopkins study, found that the Diebold system, as implemented in the state, had serious security flaws. The report concludes overall that this voting system, "as implemented in policy, procedure, and technology, is at high risk of compromise" and made many recommendations for improvements.[28] The Maryland State Board of Elections has developed a plan to implement those recommendations.[29]

The extent to which the risks identified in the Maryland study may apply to other states or to other DREs may be worth examination by state officials. In Ohio, which has also been considering the purchase of Diebold DREs, secretary of state

---

[23] (...continued)
February 2003, [http://www.scoop.co.nz/mason/stories/HL0302/S00052.htm].

[24] Hopkins study, p. 3.

[25] Diebold Election Systems, "Checks and balances in elections equipment and procedures prevent alleged fraud scenarios," 30 July 2003, 27 p., [http://www2.diebold.com/checksandbalances.pdf] (Diebold rebuttal).

[26] Rebecca Mercuri, "Critique of 'Analysis of an Electronic Voting System' document," 24 July 2003, [http://www.notablesoftware.com/Papers/critique.html]; Douglas W. Jones, "The Case of the Diebold FTP Site," updated regularly, [http://www.cs.uiowa.edu/~jones/voting/dieboldftp.html].

[27] Science Applications International Corporation (SAIC), "Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes" (redacted), SAIC-6099-2003-261, 2 September 2003, [http://www.dbm.maryland.gov/DBM%20Taxonomy/Technology/Policies%20&%20Publications/State%20Voting%20System%20Report/stateVotingSystemReport.html] (Maryland study).

[28] Maryland study, p. 10.

[29] Linda H. Lamone, "State of Maryland Diebold AccuVote-TS Voting System Security Action Plan", 23 September 2003, [http://www.elections.state.md.us/pdf/voting_system_security_action_plan.pdf].

Kenneth Blackwell has also initiated a security evaluation of electronic voting devices from four vendors.[30]

Analysis of the Problem

Elections are at the heart of the democratic form of government, and providing sufficient security for them is therefore critical to the proper functioning of a democracy. There has been some disagreement among experts about the seriousness of the potential security problems with DREs and, therefore, what is needed to ensure sufficient security. While it is generally accepted that tampering is possible with any computer system given enough time and resources, some experts believe that current security practices are adequate. Others believe that substantial additional steps are needed. To determine the nature and extent of the problem and what solutions might be considered requires an understanding of some general concepts in computer security, which are discussed in this section, along with their applicability to computer-assisted voting systems. The discussion is organized along four themes: threats, vulnerabilities, defense, and response and recovery after an incident occurs.

The term *threat* can be used in several different ways, but in this report it refers to a possible attack — what *could* happen. Descriptions of threats often include both the nature of the possible attack, those who might perpetrate it, and the possible consequences if the attack is successful. *Vulnerability* usually refers to a weakness that an attack might exploit — *how* an attack could be accomplished. Analysis of threats and vulnerabilities, when combined, can lead to an assessment of *risk*. Statements of risk often combine both the probability of a successful attack and some measure of its likely consequences.[31] *Defense* refers to how a system is protected from attack. *Response and recovery* refer to how, and how well, damage is mitigated and repaired and information and functionality are recovered in the event of a successful attack.

Threats

Kinds of Attacks and Attackers. The best known type of attack on a voting system is one that changes the vote totals from what voters actually cast. Historically, such tampering has been performed by corrupt officials or partisans, one of the most famous examples being Tammany Hall in New York City, of which Boss Tweed said, "the ballots made no result; the counters made the result."[32] Sometimes, others who stood to benefit from a particular outcome would be involved, as was reportedly the case with respect to allegations of vote-buying in Indiana with money

---

[30] Office of J. Kenneth Blackwell, "Security Contracts Finalized For Voting Systems Reviews," Press Release, 30 September 2003, [http://www.sos.state.oh.us/sos/news/release/09-30-03.htm]. Vendors qualified to participate include the three largest voting system firms — Diebold Election Systems, Election Systems and Software, and Sequoia Voting Systems — plus Hart Intercivic.

[31] See Rob Buschmann, *Risk Assessment in the President's National Strategy for Homeland Security,* CRS Report RS21348, 31 October 2002.

[32] Dugger, "Annals of Democracy," p. 46.

from some of New York's "robber barons" in the presidential election of 1888.[33] The goal of such tampering would generally be to influence the final vote tally so as to guarantee a particular result. That could be accomplished by several means, such as adding, dropping, or switching votes. Many of the features of modern voting systems — such as secret balloting and the use of observers — are designed to thwart such threats.

The impact of such vote tampering depends on several factors. Two of the most important are the scale of an attack and the competitiveness of the contest. An attack would have to have sufficient impact to affect the outcome of the election. For that to happen, scale is critical. If tampering impacts only one ballot or one voting machine, the chances of that affecting the election outcome would be small. But tampering that affects many machines or the results from several precincts could have a substantial impact, although it might also be more likely to be detected. The scale of attack needed to affect the outcome of an election depends on what proportion of voters favor each candidate. The more closely contested an election is, the smaller the degree of tampering that would be necessary to affect the outcome.[34]

While attacks that added, subtracted, or changed individual votes are of particular concern, other kinds of attacks also need to be considered. One type of attack might gather information that a candidate could use to increase the chance of winning. For example, if vote totals from particular precincts could secretly be made known to operatives for one candidate before the polls closed,[35] the results could be used to adjust get-out-the-vote efforts, giving that candidate an unfair advantage. Another type of attack might be used to disrupt voting. For example, malware could be used to cause voting machines to malfunction frequently. The resulting delays could reduce turnout, perhaps to the benefit of one candidate, or could even cause voters to lose confidence in the integrity of the election in general. The latter might be of more interest to terrorists or others with an interest in having a negative impact on the political system generally.

An Evolving Threat Environment. The kinds of attacks described above are potential threats against any voting system. However, the growing use of information technology in elections has had unique impacts on the threat environment. It provides the opportunity for new kinds of attacks, from new kinds of attackers. As information technology has advanced and cyberspace has grown, so too have the rate and sophistication of cyberattacks in general:[36]

---

[33] S.J. Ackerman, "The Vote that Failed."

[34] A common prayer of election officials on election day is said to be "Please may it not be close!"

[35] This could potentially be done, for example, if voting or counting machines in precincts used modem connections for transmittal of tallies to the central election office, and a tamperer could use that connection before the polls closed to send results to another location.

[36] Eric Fischer, Coordinator, *Understanding Cybersecurity: A CRS Workshop,* CRS Online Video MM70048, 21 July 2003.

- The number of reported computer-security violations has grown exponentially in the past decade, from about 100 in 1989 to more than 100,000 in the first three quarters of 2003.[37]
- Potential threats may now come from many sources — amateur or professional hackers using the Internet, insiders in organizations, organized crime, terrorists, or even foreign governments. With respect to election tampering, some such attackers could benefit in traditional ways, but some, such as terrorists, might be interested instead in disrupting elections or reducing the confidence of voters in the electoral process.
- New and more ingenious kinds of malware are constantly being invented and used. There are now tens of thousands of known viruses, and the sophistication of tools used to develop and use new ones has increased.

Malware in a voting system could be designed to operate in very subtle ways, for example, dropping or changing votes in a seemingly random way to make detection more difficult. Malware can also be designed to be adaptive — changing what it does depending on the direction of the tally. It could also potentially be inserted at any of a number of different stages in the development and implementation process — from the precinct all the way back to initial manufacture — and lie in wait for the appropriate moment.

Several other kinds of attack could also be attempted in addition to malware. Among them are electronic interception and theft or modification of information during transport or transmission, modifications or additions of hardware, and bypassing system controls or misuse of authority to tamper with or collect information on software or election data.[38]

Vulnerabilities

The threats discussed above, and others, are of course only harmful potentially. Their mere existence does not in itself imply anything about the likelihood that they are a significant risk in a genuine election. To be such a risk, there must be vulnerabilities in the voting system that can be exploited. For the purposes of this report, discussion of vulnerabilities is divided into two categories — technical and social.

Technical Vulnerabilities. This category includes weaknesses stemming from the computer code itself, connection to other computers, and the degree of auditing transparency of the system.

Computer Code. In the recent public debate about the security of DREs, much of the attention has focused on the computer code. Two significant potential

---

[37] Carnegie Mellon University, CERT Coordination Center, "CERT/CC Statistics," 17 October 2003, [http://www.cert.org/stats/cert_stats.html].

[38] Rebecca Mercuri and Peter Neumann, "Verification for Electronic Balloting Systems," in *Secure Electronic Voting,* ed. Dimitris Gritzalis, (Boston: Kluwer, 2003), p. 31-42.

vulnerabilities relate to the use of cryptography in the system and the way the code is designed. Cryptography[39] is one of the most powerful tools available for protecting the integrity of data. Robust cryptographic protocols are well-developed and in common use, for example in online financial transactions. Cryptography is important not only in making it difficult for unauthorized persons to view critical information (security), but also in making sure that information is not changed or substituted in the process of being transferred (verification). This could be a concern for DREs; both the Hopkins and Maryland studies found weaknesses in the way encryption was used.

The design of software can have a significant effect on its vulnerability to malware. Both the complexity of the code and the way it is designed can have an impact. It is a general principle of computer security that the more complex a piece of software is, the more vulnerable it is to attack. That is because more complex code will have more places that malware can be hidden and more potential vulnerabilities that could be exploited, and is more difficult to analyze for security problems. In fact, attackers often discover and exploit vulnerabilities that were unknown to the developer, and many experts argue that it is impossible to anticipate all possible weaknesses and points of attack for complex software. With DREs, each machine requires relatively complex software, since it serves as a voter interface, records the ballot choices, and tallies the votes cast on the machine.[40] The first function requires the most complex software, especially if the machine is to be fully accessible to all voters. The code used in optical-scan and punchcard readers can be simpler, as it performs fewer functions.

Software code that is not well-designed from a security perspective is more likely than well-designed code to have points of attack and weaknesses that could be exploited, as well as places for malware to be hidden. However, code can be designed so as to minimize such vulnerabilities, and well-developed procedures have been established to accomplish this goal.[41] These procedures can be applied to both new and legacy systems. Good design involves not only the code itself, but also the process by which it is developed and evaluated. DRE code has been criticized with respect to its design,[42] although the proprietary nature of the software has precluded thorough public assessment. The systems may also use commercial off-the-shelf software for functions such as the operating system, and that software could also have

---

[39] *Cryptography* refers to the process and use of methods for the encoding or *encryption* of information, such as a piece of plain or clear text, so that it cannot be deciphered, and the subsequent decoding or *decryption* of that information. Cryptographic methods are used to help protect information from unauthorized access (confidentiality), prevent undetected modification (integrity), to confirm identity (authentication), and to prevent a false denial of identity (nonrepudiation) (National Research Council (NRC), *Trust in Cyberspace,* (Washington, DC: National Academy Press, 1999), p. 301–310).

[40] Caltech/MIT study, p. 60.

[41] Linger and Trammell, "Cleanroom Software Engineering." See also footnote 93.

[42] Hopkins study; Jones, "Diebold FTP Site."

vulnerabilities. However, the software in the major systems in use today has been evaluated and certified as meeting VSS requirements, including those for security.[43]

Connection to Other Computers. This can be a vulnerability because it provides potential avenues for attack. The most well-known attack targets are computers with direct Internet connections that hackers can exploit. Concerns about such attacks have made the adoption of Internet voting in public elections generally unattractive so far from a security perspective.[44] While a measure of protection can be provided by firewall programs and related technology, the safest approach is to ensure that the voting system computers, including not just the voting machines themselves but also computers involved in ballot generation and vote tallying, are not connected to the Internet or to any other computers that are themselves connected to the Internet. This isolation is sometimes called "air-gapping." However, an effective air gap must include sufficient security controls for removable media such as floppy disks,[45] CDs, and the memory cards that are often used to transport data from the precinct to the central election office.[46]

Vendors and election jurisdictions generally state that they do not transmit election results from precincts via the Internet, but they may transmit them via a direct modem connection. However, even this approach can be subject to attack via the Internet, especially if encryption and verification are not sufficient. That is because telephone transmission systems are themselves increasingly connected to the Internet (as exemplified, for example, by the increasing use of Internet-based telephony), and computers to which the receiving server may be connected, such as through a local area network (LAN), may have Internet connections. In fact, organizations may be unaware of the extent of such connections.[47] This can be even more of an issue if the system uses wireless connectivity.

The way that a voter interacts with the DRE may provide another possible source of connection. For example, with the Diebold DRE, a "smartcard"[48] is inserted into the voting machine to start the voting process (some machines use other methods, such as a numerical code). The Hopkins study claims that voters or pollworkers could program their own smartcards and use them to vote repeatedly or to manipulate the voting machine. The Diebold rebuttal rejected this assertion. The Maryland study, while not ruling out this vulnerability, states that software and

---

[43] NASED, "Voting Systems That Are NASED Qualified," 3 January 2003, [http://www.nased.org/NASEDApprovedSystems1.03.pdf]. See also Britain J. Williams, "Security in the Georgia Voting System," 23 April 2003, available at [http://www.votescount.com/georgia.pdf].

[44] See Kevin Coleman, *Internet Voting,* CRS Report RS20639.

[45] Computer viruses were originally spread through floppy disks.

[46] This need applies to any computer-assisted voting system with precinct tabulation.

[47] Fischer, *Understanding Cybersecurity Workshop.*

[48] A *smartcard* is a card, usually about the size of a credit card, with an embedded computer chip that can communicate with another electronic device that can read information from and/or write it to the card.

physical controls, and the openness of the voting booth,[49] minimize the likelihood of exploitation.

Auditing Transparency. In current DREs, the actions that occur between ballot screen and the final vote tally are not subject to human observation. The voter sees a visual representation of the ballot on the computer screen or face of the DRE. When the voter pushes the button to cast the ballot, the machine records the votes electronically. That means that a voter cannot know if the machine recorded the choices the voter saw on the screen or some other choices, and an observer also cannot check to see if all ballots cast are counted correctly. The former vulnerability also exists with a mechanical lever machine, and the latter with an optical scan or punchcard ballot reader, but with a reader, there is a document ballot that can be checked independently. While DREs are generally designed to make a separate recording of each ballot cast,[50] this is not an independent record but rather a copy in a different format of the information sent to the tallying registers.

Social Vulnerabilities. A significant and increasingly sophisticated kind of attack — dubbed "social engineering" by hackers — involves finding and exploiting weaknesses in how people interact with computer systems.[51] Such social vulnerabilities can include weaknesses relating to policy, procedures, and personnel. Of the 14 specific risks identified in the Maryland study, most were of these types.[52]

Policy. A security policy lays out the overall goals and requirements for a system and how it is implemented, including the technology itself, procedures, and personnel.[53] An absent or weak policy, or even a good one, if it is not implemented, is considered a substantial vulnerability. Security policies of election administrators,

---

[49] Use of illegitimate smartcards could be difficult with certain common election administration practices — for example, if a pollworker, rather than the voter, inserts the smartcard into the DRE; if the voting booth is not fully screened and pollworkers observe the behavior of voters for irregularities; and if time limits for voting are enforced. However, voters may legitimately be concerned with privacy when they cast their votes and may try to obscure the view of others, and pollworkers, in the interest of protecting the voter's privacy, may be reluctant to watch closely enough to detect attempts to use an illegitimate card.

[50] Systems that conform to the VSS are required to have this function (FEC, *Voting Systems Performance and Test Standards,* Sec. 2, p. 4).

[51] For example, one kind of attack involves sending victims email purportedly from a legitimate financial or software company and urging them to visit a website, also purportedly of this company, where they are requested to enter information such as a usernames and passwords for accounts. The hacker can then use this information to take control of the victim's computer or to steal funds.

[52] However, two of the risks are entirely redacted. References in this and other sections to weaknesses found in Maryland's implementation of the Diebold system are made because this was the only system for which an independent analysis of such weaknesses was available. It is not intended to imply in any way that Maryland or the Diebold system exhibit more or more serious vulnerabilities than other states or systems.

[53] The SANS Institute, "A Short Primer For Developing Security Policies," 6 October 2001, [http://www.sans.org/resources/policies/Policy_Primer.pdf].

vendors, third-party suppliers, and the ITAs are all relevant. The Maryland study found that the Diebold system as implemented did not comply with the state's information security policy and standards. The study did not examine the security policies of Diebold or other relevant entities.

Procedure. The security policy provides the basis from which procedures such as access controls are developed. Election administration is a complex effort involving vendors, ITAs, state and local government, and pollworkers who are often volunteers, as well as voters. Also, DREs are potentially targets of attack at virtually any point from when they are initially developed and manufactured to when they are used in the polling place. Consequently, security procedures are especially important. Vulnerabilities can occur, for example, if the controls that the manufacturer uses to prevent insertion of malware are inadequate; if the analyses performed by evaluators is not sufficient to detect security problems with the technology; if the chain of custody for software, including updates — from when it is certified to when it is used in an election — is weak or poorly documented; or if auditing controls are insufficient. As with security policy, absent or poor procedures, or even good ones if they are not properly implemented, can create serious vulnerabilities. The Maryland study did not examine vendor or ITA practices[54] but did raise several concerns with respect to the procedures used by the state.

Personnel. Perhaps the most important single factor in determining the vulnerability of a system is the people involved. It is they who must implement security policies and procedures and defend against any attacks. If they are not adequately skilled and trained, they may be unable to prevent, detect, and react to security breaches, and they may themselves be more vulnerable to a "social engineering" attack. In addition, it can be particularly difficult to defend against attack by an insider, so background checks and other controls to minimize that risk are especially important. The Maryland study pointed out that the state training program for the Diebold system did not include a security component.

Defense

Goals of Defense. It can be useful to think of three goals of defense from an attack on a computer-based system: protection, detection, and reaction.[55] *Protection* involves making a target difficult or unattractive to attack. For example, good physical security can prevent attackers from accessing voting machines in a warehouse. Use of encryption and authentication technologies can help prevent attackers from viewing, altering, or substituting election data when it is transferred.

---

[54] Some others, however, have raised concerns or suggested improvements to vendor and ITA practices (see, for example, the Hopkins study [cf. Diebold rebuttal]; Jones, "Diebold FTP Site"; and the California Task Force report).

[55] National Security Agency (NSA), "Defense in Depth: A Practical Strategy for Achieving Information Assurance in Today's Highly Networked Environments," NSA Security Recommendation Guide, 8 June 2001, available at [http://nsa2.www.conxion.com/support/guides/sd-1.pdf]. *Deterrence* may be used by some authors instead of *reaction.*

Currently, election jurisdictions and vendors appear to rely heavily on procedural mechanisms for protection.[56] These may include access controls, certification procedures, pre-election equipment-testing, and so forth. Such procedures are an essential element of an effective defense, although some observers dispute that they are sufficient to prevent tampering. Even if they are, they must be implemented and followed properly if they are to ensure adequate protection. However, in some circumstances, the time and resources needed to follow such procedures may conflict with other important goals, such as the timely administration of an election, forcing election officials to choose whether to risk bypassing or modifying security procedures.[57]

Detection involves identifying that an attack is being or was attempted. For example, election observers can serve as detectors of a potential attack. One of the criticisms of DREs has been that it is a "black box" system, and observers cannot detect suspicious activity within the machine.[58] One approach to addressing this issue is the use of auditing. That can include engineering the DRE so that it creates a log of all actions performed, especially those that might indicate tampering. It can also include the creation of an audit trail for votes. HAVA requires such a trail for the voting system, but some observers have proposed the use of voter-verified ballots for auditing (discussed below[59]). Cryptographic protocols may also be useful in detecting attempts at tampering.[60] However, any specific mechanisms that might be built into the technology itself are proprietary and therefore not discussed in this report.

Reaction involves responding to a detected attack in a timely and decisive manner so as to prevent its success or mitigate its effects. For example, if an observer sees something suspicious during voting or tallying, the process can be stopped and the situation investigated. Also, a voting machine may be programmed to shut down if certain kinds of problems are encountered. The system might have additional defense measures such as antivirus software.

To be most effective, the countermeasure must be implemented before the attacker can do significant damage. Effective reaction therefore requires early detection of an attack. Given the lack of transparency of DRE operations, heavy reliance may need to be placed on technological countermeasures.

---

[56] See, for example, the Diebold rebuttal and the Maryland study.

[57] For example, if a serious software problem is discovered shortly before an election, officials might have to choose whether to have a vendor install a patch directly, without having it first certified through ITA and state procedures.

[58] See section on auditing transparency above, p. 15.

[59] See section on verifiability, p. 27–31.

[60] See section on computer code above, p. 13

Elements of Defense. It is generally accepted that defense should involve a focus on three elements: personnel, technology, and operations.[61] The *personnel* component focuses on a clear commitment to security by an organization's leadership, assignment of appropriate roles and responsibilities, implementation of physical and personnel security measures to control and monitor access, training that is appropriate for the level of access and responsibility, and accountability. The *technology* component focuses on the development, acquisition, and implementation of hardware and software. The *operations* component focuses on policies and procedures, including such processes as certification, access controls, management, and assessments.

A focus that is not properly balanced among those elements creates vulnerabilities. Computer security experts have criticized computer-assisted voting in part because they believe that the security focus has emphasized procedural safeguards too heavily. The use of older, "legacy" hardware and software technology, and weak technology defenses, as well as lack of training of election personnel in security, are among the concerns experts have cited. The validity of such concerns has been disputed by others.[62]

For applications where security considerations are a priority, techniques have been developed to engineer systems to the appropriate level of security corresponding to the specific needs for the application. Such systems are designed with carefully specified requirements and are thoroughly reviewed and tested before implementation.[63] Some experts have proposed that such an approach be used in the development of voting systems.[64]

Another general principal is that an effective defense cannot be focused only on one particular location but needs to operate at all relevant points in the entire enterprise.[65] For voting systems, these points would likely include development (both software and hardware) by the manufacturer, the certification process, acquisition of the voting system (including software and hardware updates) by the state, state and local implementation, and use during elections. Because of the proprietary nature of vendor practices, the defenses used by them could not be

---

[61] NAS, "Defense in Depth."

[62] For example, see the Caltech/MIT, Hopkins, and Maryland studies, the California Task Force report, and Jones, "Diebold FTP Site" for criticisms and recommendations for improvements; and for alternative views, see the Diebold rebuttal and Williams, "Georgia Voting System."

[63] See, for example, Linger and Trammell, "Cleanroom Software Engineering"; and Syntegra, "Common Criteria: An Introduction," 21 February 2002, available at [http://www.commoncriteria.org/introductory_overviews/CCIntroduction.pdf].

[64] Rebecca Mercuri, "Electronic Voting," 1 September 2003, [http://www.notablesoftware.com/evote.html].

[65] NSA, "Defense in Depth."

determined for this report.[66] State procedures are more transparent in many cases but vary from state to state.[67]

Finally, an effective defense is based on the assumption that attackers will continuously attempt to breach the defenses (including devising new ways to attack) and that they will eventually find a vulnerability to exploit. Therefore, a successful defense should be *robust,* so that security needs are met even if an attack occurs.[68] One way to accomplish this is through a *layered defense,* in which more than one defense mechanism is placed between the attacker and the target.[69] If the outer layer is breached, the next comes into play. Each layer should include both protection and detection capability. For example, a state will use a combination of physical security (e.g., lock and key), procedural controls (e.g., who is given access to the system and for what purpose) and auditing (a record of what was done and by whom) to defend against tampering with voting systems. Georgia does additional validation testing on software installed on machines in a local election jurisdiction to ensure that it is the same as the certified software.[70] Other states may have similar procedures.

Trade-Offs. The combined use of goals and elements as discussed above is known as *defense in depth.* Such a strategy requires balancing "protection capability and cost, performance, and operational considerations."[71] This balancing can involve difficult questions, especially with regard to resource allocation. For example, how much effort should be expended in threats that may have a significant probability but a comparatively low impact versus addressing those with very low probability but very high impact? The need to weigh such trade-offs occurs throughout the security arena. In the area of homeland security, the number of casualties from a terror attack using the smallpox virus could be much higher than from an attack with explosives, but the latter is widely considered much more likely. Furthermore, there are many other factors that must be weighed, such as balancing protection against the threat, on the one hand, against the safety of countermeasures (such as vaccines) and disruption to daily life (such as screening for explosives) on the other.

Setting priorities with respect to investment in defense in such cases is far from straightforward. This is true for election administration as well. Decisions about what kinds of security to provide and how to provide it must be made in complex circumstances. For example, with DREs, the probability of successful tampering occurring may be very small, but the impact of a successful attack could be very high.

---

[66] Diebold claims that its security procedures make insertion of malware during development "realistically impossible" (Diebold rebuttal, p. 6). The California task force report makes several recommendations with respect to vendor security, including requiring background checks of programmers and developers and documentation of the custody chain for software (p. 36).

[67] Williams, "Georgia Voting System," describes Georgia's certification procedures. The Maryland study made several recommendations for improvements in state procedures.

[68] See, for example, Burmester and Magkos, "Toward Secure and Practical E-Elections".

[69] NSA, "Defense in Depth."

[70] Williams, "Georgia Voting System."

[71] NSA, "Defense in Depth," p. 1.

At the same time, current DREs arguably reduce the risks of certain kinds of tampering that can occur with paper ballots — such as selectively spoiling certain ballots during counting. Many DREs also have other highly desirable features, as discussed earlier,[72] that can substantially reduce the number of votes lost because of voter error or other problems. According to one study, over a million of such "lost votes" could have been prevented during the November 2000 presidential election if better-designed voting technology had been used.[73]

Also, security measures may have unanticipated impacts. Measures that made voting much more difficult or complicated and thereby discouraged voters from participating or increased the rate of voter or pollworker error would probably not be worth implementing. Furthermore, voting machines are only part of the election administration system, and security must be integral to the whole system to be effective.

Response and Recovery

The idea that no defense is perfect and that attackers try to find the imperfections means that defenders need to assume that an attack will at some point be successful. Some damage will occur before the attack is detected and stopped (assuming that the attack is detected — in the case of vote tampering, an attacker would usually prefer that the attack not be discovered and will make efforts to hide it[74]). For this reason, mechanisms for minimizing and recovering from damage that occurs are considered desirable. They are also desirable in the event of damage that can result from sources other than an attack, such as power outages, malfunctioning voting machines, or administrative problems. For example, DREs store vote data in redundant memory locations, in the event that one memory fails. As the difficulties with spoiled ballots from the November 2000 Presidential election indicated,[75] recovery from some kinds of damage may not be possible, and reliance must be placed on strengthening preventive measures. Thus, HAVA requires that voters be notified of overvotes before a ballot is cast and be given the opportunity to correct errors.[76]

One criticism of DREs has been that if a problem is discovered during auditing, it is not clear what can be done to identify which votes were valid and which were not. For example, if a machine is suspected of harboring malware, should all votes

---

[72] See page 4.

[73] Caltech/MIT report, p. 8–9.

[74] For example, in a statewide election, increasing the votes for a candidate in a precinct already voting heavily for that person may be less likely to trigger questions than would changing the vote in a closely fought precinct.

[75] In this case the problems arose from ballot design and procedural flaws rather than an attack.

[76] However, for systems where this is not possible — such as those using document ballots where votes are not counted in the precinct but in a central location — an education and instruction program is permitted.

from it be discarded, or would some be counted? How election officials answer such questions will depend on state law, regulations, and practices.

One mechanism for recovery from some kinds of problems is the recount, in which ballots are counted a second time to address concerns about the accuracy of the original count. DREs, like lever machines, simplify recounts and reduce chances for error in them because the recounts are based on the vote tallies from the machines, rather than individual ballots. However, problems with the machines themselves, including tampering, would probably not be discovered through a recount.

Confidence in DREs

There appears to be an emerging consensus among computer scientists that current DREs, and to a lesser extent other computer-assisted voting systems, do not adhere sufficiently to currently accepted security principles for computer systems, especially given the central importance of voting systems to the functioning of democratic government.[77] However, election administrators and those with related expertise tend to express more confidence in the systems as they are currently realized.[78] Also, the fact that security concerns exist does not in itself mean that voting systems have been compromised or are likely to be. It does, however, suggest that the issues raised need to be addressed expeditiously, especially given the evolving threat environment and vulnerabilities discussed above.

The question of confidence in computer-assisted voting systems is important in general, since voters must have confidence in the integrity of the voting systems they use if they are to trust the outcomes of elections and the legitimacy of governments formed as a result of them. If the concerns that have been raised about DRE security become widespread, that confidence could be eroded, whether or not those concerns are well-founded. This potential problem could be exacerbated by two factors. One is the likelihood, especially given the applicable provisions of HAVA, that the use of DREs will increase. The other is the likelihood of increasing concentration of market share for voting systems in a few companies.[79] Historically, election jurisdictions in the United States have used a wide diversity of voting systems provided by a broad array of vendors. This diversity has been considered an advantage by many, not only in meeting the diverse needs of election jurisdictions, but also for security, especially in statewide and federal elections where more systems may be used. Some experts believe that it is much more difficult to successfully commit widespread tampering with elections if many different systems

---

[77] See the Caltech/MIT study, the California Task Force report, the Hopkins study, and the Maryland study.

[78] See for example Williams, "Georgia Voting System"; The Election Center, "DREs."

[79] According to Diebold, the combined U.S. market share for the three largest voting system companies — Diebold Election Systems, Election Systems and Software, and Sequoia Voting Systems — increased from 74% in 2000 to 89% in 2002 (Gregory Geswein, Senior Vice President and Chief Financial Officer, Diebold, Incorporated, Untitled presentation slides, 24 February 2003, [http://www.diebold.com/investors/presentation/ir2003.pdf], p. 21).

need to be compromised than if only a few must be. In any case, as the usage of DREs increases, they and the companies that make and sell them may be subjected to increased public scrutiny.

For these and other reasons, many experts and observers have proposed actions to resolve the controversy over DRE security. Several of these ideas are discussed below.

Proposals for Resolving the Issue

Use Current Procedures

Some observers have argued that existing security mechanisms are sufficient to resolve any problems and that no new solutions are necessary, although current procedures may need to be improved, as recommended by the Maryland study.[80] These observers argue that the federal Voting System Standards (VSS); NASED, state, and local certification processes; and vendor and election administration procedures and controls, when properly implemented, provide sufficient security to prevent tampering. They also point to the lack of any proven case, despite many accusations, of election fraud involving computer tampering,[81] and that criminal penalties provide a deterrent to election fraud.[82] Critics state, in contrast, that those processes and procedures are flawed, and that recommended or stated security procedures are not always followed. They also point out that the absence of a proven case of tampering does not necessarily mean that it has not been attempted, and that as the usage of DREs increases, the potential payoff for tampering, and hence the potential threat, will also increase.[83]

---

[80] See for example, the Diebold rebuttal and Lamone, "Action Plan."

[81] The occurrence of voter error or machine malfunction is sometimes pointed to as evidence for vote fraud, but they are not the same. However, both fraud and error can affect the outcome of an election, and both need to be minimal to ensure the integrity of the results. In addition, if errors occur frequently, they could mask an occurrence of fraud — if a discrepancy is discovered, officials might simply conclude that it is another case of error even if it is actually caused by tampering. See also footnote 122.

[82] Federal law prohibits voting more than once (42 U.S.C. § 1973i(e)), vote buying and selling (18 U.S.C. § 597, 42 U.S.C. § 1973i(c)), and procuring, casting, or tabulating fraudulent ballots (42 U.S.C. § 1973gg10(2)). The Public Integrity Section of the Voting Rights Division of the Department of Justice prosecutes such cases.

[83] See, for example, Bev Harris, *Black Box Voting* (High Point, North Carolina: Plan Nine Publishing, 2003), available at [http://www.blackboxvoting.com].

Improve Security Standards and Certification of Voting Systems

Some critics have stated that the security provisions in the VSS are insufficient,[84] and that their development did not follow best practices in this area, as promulgated and practiced, for example, by national and international standards-setting organizations such as the American National Standards Institute (ANSI), the International Organization for Standardization (ISO), and NIST, which has been involved only marginally in the development and implementation of the VSS.[85] The VSS have also been criticized for placing too many constraints on the development of new technology that can address security concerns.[86] Critics also point out that several of the problems identified by the Hopkins and Maryland studies occurred despite the certification by NASED that the Diebold system conforms to the VSS.

HAVA requires changes in the processes for developing standards for and certifying voting systems. It establishes a Technical Guidelines Development Committee under the new Election Assistance Commission to assist the EAC in the development of voluntary voting system guidelines. These guidelines will essentially replace the current Voluntary Voting System Standards (VSS), but the Act also stipulates that the initial set of guidelines will be the most recently adopted version of the VSS. The new Committee established by HAVA will be chaired by the Director of NIST and will include, among others, representatives of ANSI, the Institute of Electrical and Electronics Engineers (IEEE), and NASED. IEEE has already begun developing new draft voting system standards.[87] These standards would presumably be used to help inform the guideline-development process once the EAC and its support bodies are established.

The importance of standards was reinforced with the initial adoption and implementation of the VSS, which led to significant improvements in computer-assisted voting systems. Standards are essential to security because they specify measurable attributes a system needs to be considered trustworthy, and they can reduce design flaws.[88] However, a particular challenge that arises with respect to security standards is that it is not possible to anticipate all the ways a system might be attacked. In addition, standards can provide adversaries with information they can

---

[84] For example, Mercuri and Neumann, "Verification," p. 37.

[85] For some legislative history of the development of the VSS, see Eric Fischer, *Federal Voting Systems Standards: Congressional Deliberations,* CRS Report RS21156, 25 February 2002.

[86] For example, the DRE standards assume that the voter interface and the vote tallying components will be in the same unit, which may constrain manufacturers from following one of the central security-related recommendations of the Caltech/MIT report (p. 72), which is to separate those functions in different units.

[87] IEEE, "Standards Coordinating Committee 38 (SCC 38): Voting Standards," accessed 8 October 2003, [http://grouper.ieee.org/groups/scc38/index.htm].

[88] NRC, *Trust in Cyberspace,* p. 201, 209.

use in searching for vulnerabilities.[89] Therefore, security standards need to be continually reevaluated as new threats and vulnerabilities are discovered. Also, it is considered risky to treat adherence to standards as an indication that a system is secure.[90] The federal government requires that federal agencies adhere to a set of computer-security policies, standards, and practices,[91] but these do not apply to voting systems, which are under the purview of state and local governments.

Standards can be difficult and time-consuming to develop, especially under the commonly used consensus approach, in which stakeholders reach agreement on provisions to be included. Strengths of this approach, when properly implemented, are that the resulting standards are less likely to contain substantial omissions, and they are more likely to be acceptable to users and other stakeholders. Efforts to develop the VSS began in the 1970s, but the standards were not approved until 1990.[92] The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408), which is a set of requirements for evaluating the security of information technology, took five years to develop, efforts having been begun in 1993 and completed in 1998.[93] The IEEE voting standards project began in 2001 and has proceeded amid some controversy, which apparently is not atypical for standards panels addressing difficult issues.[94] Given those considerations and the delays in establishing the EAC, it is not clear whether new standards or guidelines will be in place before the HAVA voting system requirements go into effect in January 2006; however, HAVA requires the Technical Guidelines Development Committee to

---

[89] Ibid., p. 209. Although there are many benefits from having a single, uniform set of standards, that does have the potential for increasing vulnerability in the sense that "...it is easier to mount attacks against multiple representatives of a single standard than against differing implementations of several standards" (Ibid., p. 204). This is somewhat analogous to the vulnerabilities associated with use of a single, uniform voting system (see above).

[90] Ibid., p. 203.

[91] See Marcia Smith and others, *Internet: An Overview of Key Technology Policy Issues Affecting Its Use and Growth,* CRS Report 98-67, 11 July 2003, p. 9-11.

[92] There were several factors involved in this delay. See Fischer, *Federal Voting System Standards.*

[93] Edward Roback, Chief, Computer Security Division, National Institute of Standards and Technology, "Exploring Common Criteria: Can it Ensure that the Federal Government Gets Needed Security in Software?" testimony before the House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, 17 September 2003. The notion of criteria is broader than that of standards because it generally includes things, such as statements on how a system should be designed and operated, that cannot be directly assessed by examining the product (National Research Council, *Trust in Cyberspace,* p. 199). The Common Criteria provide a framework for the development of standard sets of requirements, called profiles, to meet specific needs of consumers and developers, depending on the assurance level that they require (Syntegra, "Common Criteria"). HAVA uses the term guidelines rather than standards or criteria and does not define it.

[94] Farhad Manjoo, "Another case of electronic vote-tampering?" *Salon.com,* 6 October 2003, [http://archive.salon.com/tech/feature/2003/09/29/voting_machine_standards/index_np.html]

submit its initial recommendations to the EAC within nine months of the Committee's appointment.[95] In any case, even after new standards are approved, there remain issues relating to testing and certification. For example, should all voting systems be required to adhere to the new guidelines or should those certified under the VSS continue to be accepted?

The current process for testing and certification of voting systems was initiated by NASED in 1994. HAVA directs the EAC to provide for "testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories" (Sec. 231(a)(1)). It gives NIST responsibility for recommending and reviewing testing laboratories.

While HAVA maintains the voluntary nature of adherence by states to federal voting system standards and use of certified systems, most states have adopted the VSS.[96] Consequently, if the EAC decertifies voting systems that do not meet the new guidelines, many states would likely replace those systems, provided that funding were available to do so. However, the more stringent a set of standards is with respect to security, the more time-consuming and expensive it may be to test and certify the system (some have criticized the Common Criteria for this reason, although others have suggested that they be applied to voting systems[97]). More secure systems may also be more expensive to manufacture. Consequently, there may be economic disincentives for investment in highly secure voting systems, although such disincentives would likely become less important if public concern grows.

Under the current VSS, testing is performed under specific laboratory test conditions. Such tests are necessary to determine if the system meets the standards, but some experts have proposed that they are not sufficient, that additional testing needs to be done under realistic conditions of use, involving actual voters, and that systems should be retested after use in the field.[98]

Even if new guidelines and certification procedures can be developed that include state-of-the-art security features, some observers believe that this will not be sufficient. They point to three problems: (1) Given the time required to develop and implement new voting system guidelines and to test and certify systems under them, systems reflecting such guidelines will not be in place for several years, whereas the threat from cyberattacks is present and growing. (2) Overreliance on any one line of defense, such as security standards, runs counter to the recommended use of defense in depth. (3) The use of standards does nothing about the reduced observability and

---

[95] HAVA distinguishes between the *guidelines* (Sec.221-222), which replace the VSS, and *guidance* (Sec. 311-312) for meeting the requirements of the Act. The deadline for adoption of guidance for meeting voting system requirements is January 2004.

[96] FEC, *Voting Systems Performance and Test Standards: An Overview,* p. 15.

[97] Rebecca Mercuri has recommended that voting systems be benchmarked at level 4 or above of the 7 levels (Mercuri, "Electronic Voting").

[98] See Caltech/MIT report, p. 72-73.

transparency that characterizes computerized voting systems[99] in contrast to more traditional systems, and therefore cannot sufficiently address concerns about public confidence in the integrity of computer-assisted voting. Some experts also believe that certification and procedural controls, including auditing, can never guarantee security of a voting system.[100] This problem, they say, is further complicated by the need for ballot secrecy, which is not an issue, for example, in computerized financial transactions.

Use Open Source Software

Some experts have proposed the use of *open source* software code for at least some voting system software.[101] Such code would be available for public inspection and undergo thorough security review, and these experts argue that it would therefore be more secure because the open source review process would be more thorough and identify more potential security flaws than is possible with proprietary code. Advocates of proprietary or *closed source* code argue, in contrast, that this approach makes potential flaws more difficult to discover and therefore to exploit. Even if open source code is superior with respect to security (which remains unproven), DREs often use commercial off-the-shelf (COTS) software (such as Microsoft Windows) that is proprietary.[102]

Currently, the code for virtually all voting system software in the United States is closely held by the vendors, who release it only to select parties, such as the ITAs, under nondisclosure agreements. The vendors argue that the use of proprietary software is important both to protect their intellectual property rights and for security. While secrecy can be an important security tool (sometimes called "security through obscurity"), it has some weaknesses. First, it is fragile, in that once this defense is breached, the damage cannot be repaired — the code cannot be made secret again. Second, use of secrecy limits the number of people who can examine the code, thereby limiting the scrutiny it can receive for vulnerabilities. Both of these potential weaknesses were demonstrated by the circumstances leading to the Hopkins study. Diebold code was posted (perhaps inadvertently) on an open Internet server; the authors analyzed this code and claimed to have discovered several vulnerabilities (which Diebold disputed).

---

[99] Some advocates pejoratively refer to DREs as "black-box voting" (see for example, [http://www.blackboxvoting.com/]).

[100] See, for example, Mercuri and Neumann, "Verifiability," p. 39.

[101] "Open source software refers to a computer program whose source code is made available to the general public to be improved or modified as the user wishes" (Jeffrey W. Seifert, *Computer Software and Open Source Issues: A Primer,* CRS Report RL31627, 5 November 2002, p. 1). What is "open" (or "closed") is the source code — what programmers actually write. This code is translated into machine code (compiled) for use by computers to run the programs. Machine code can be translated back into source code (decompiled). This does not recover the original source code but can be useful, for example, to hackers hoping to find vulnerabilities, or to defenders looking for malware that might be in the machine code.

[102] The way COTS software is tested and used in current DREs might itself create vulnerabilities (Jones, "Diebold FTP Site").

Some have proposed resolving this issue by using a modular approach that separates the voter interface or ballot choice function (equivalent to marking an optical-scan ballot) from the vote-casting function (putting the ballot in the optical-scan reader).[103] The software for the latter would be open source and standardized and for the former proprietary and more flexible. The reasons are that vote casting is a straightforward, well-defined process that requires high security to ensure that the voter's actual choices are recorded and counted, whereas the voter interface is where innovations can provide the greatest advances in usability and other benefits for voters, and the security requirements are not as stringent. The code used for vote casting and counting can be much simpler than that needed for the voter interface, making security potentially much easier to achieve than is currently the case with DREs, where both functions are housed within a single unit.

Improve Verifiability and Transparency

Verifiability in elections can be thought of as consisting of two components. One involves the capability of the voter to verify that his or her ballot was cast as intended. This is what is usually meant by *voter verifiability*. The other involves the capability to determine that the final tally accurately reflects all votes as cast by the voters and that it includes no additional votes — in other words, that no votes were improperly changed, omitted, or added. This has been called *results verifiability*.[104] If all voters can obtain both voter and results verifiability, that is known as *universal verifiability*.[105] Roll-call voting provides robust universal verifiability — voters publicly record their votes, which are counted in the presence of all voters. However, this approach sacrifices ballot secrecy and can be used only for very small electorates. While ballot secrecy reduces the risk of vote selling and coercion, it complicates verifiability, since voters cannot know directly if their ballots were counted as cast. Hand-counted paper ballot systems, which can provide ballot secrecy, may provide universal verifiability only under some very limited circumstances and only for very small electorates. Such systems can provide a kind of surrogate results verifiability, if observers closely watch the counting of ballots, but even that can be difficult to achieve. Lever machines and computer-assisted voting systems arguably exhibit neither voter nor results verifiability, although document-based systems such as optical scan and punchcards do retain the capacity for surrogate results verifiability if manual recounts are done in the presence of observers.

Some observers believe that the potential security problems associated with the lack of transparency and observability in vote casting and counting with DREs cannot be resolved through the use of security procedures, standards, certification, and testing. They assert that the only reliable approach is to use ballots that voters can

---

[103] Caltech/MIT report, p. 60, 63. The authors further propose that these be performed by different machines. See the section on modular voting architecture, p. 29, for a description of this approach.

[104] See C. Andrew Neff and Jim Adler, "Verifiable e-Voting," 6 August 2003, [http://www.votehere.net/vhti/documentation/verifiable_e-voting.pdf].

[105] Mike Burmester and Emmanouil Magkos, "Toward Secure and Practical E-Elections in the New Era," in Gritzalis, *Secure Electronic Voting*, p. 63-76.

verify independently of the DRE and that these ballots become the official record for any recounts. Others assert that voter verifiability is a highly desirable feature but caution about some of the proposed ways of achieving it. Still others believe that there are problems with the approach that make it undesirable.

HAVA requires that each voting system produce a paper audit record for the system and that this be the official record for recounts. It also requires that voters have the opportunity to correct their ballots before that record is produced. However, it does not stipulate that that record consist of individual ballots or that it be verifiable by the voter.

At least four different ways of achieving voter verifiability have been proposed. These are discussed below to illustrate the range of complexity and issues involved.

Voter-Verifiable Paper Ballot. In the most widely discussed method, the DRE would print a paper ballot with the voter's choices listed. The voter could then verify that the ballot accurately reflected the voter's choices as made on the DRE. Any discrepancies could then be called to the attention of a pollworker. Once the voter was satisfied with the paper ballot, it would be deposited in a ballot box[106] and kept in the event of a recount. A sample of these ballots could also be counted as part of a standard audit for comparison with the total count. Some observers also believe that any recount using these paper ballots should be performed by hand rather than machine.

This approach has the following potential advantages: (1) Any recount would be based on an independent record that the voter had had an opportunity to verify. (2) Each election could be audited, and any significant discrepancies between the electronic and paper tallies would trigger a full recount. (3) If the recount were performed by hand, that would take advantage of the transparency and observability that can be associated with that approach. (4) The method could help ensure voter confidence in the legitimacy of election results, since voters would know that ballots they had verified would be available for recounts.

The approach has also been criticized, with critics asserting the following: (1) It makes voting more complicated and time-consuming by requiring extra steps by the voter. (2) The use of printers would substantially increase both the cost of administering an election and the risk of mechanical failure of a voting machine. (3) It is generally accepted that paper ballot systems cannot be made to conform to the

---

[106] This could be done by the voter or by the DRE (the voter need not handle the ballot but could view it through a transparent pane (see Rebecca Mercuri, "A Better Ballot Box?" IEEE Spectrum Online, October 2002, [http://www.spectrum.ieee.org/WEBONLY/publicfeature/oct02/evot.html]), although the latter approach could raise issues about ballot secrecy if the ballots were deposited in the box in the order in which voters used the DRE (ballots are not recorded in the order cast in the DRE's memory). The method as usually described does not provide voters with ballot "receipts" that they can take from the polling place, which would create significant opportunities for fraud and abuse, if those receipts showed the choices the voter made.

HAVA accessibility requirements.[107] (4) Since the method is largely untested, it is not clear to what extent it would improve security in practice and what impacts it might have on voters.[108] (5) Hand counting of the paper ballots would be time-consuming and arguably more error-prone than machine counting.[109]

Votemeter. There is an electronic version of the above method, in which an electronic device would be attached to the DRE. This *votemeter* would have a display on which the voter could verify choices and it would record those choices independently of the DRE. Those records would be used in any recount and could also be tallied separately by an independent agency — to provide a check on possible collusion with respect to the DREs. Advantages to such a system over a paper trail would be that it would not have the problems of manual paper recounts, it could provide a fast, independent, full audit of the DRE vote, and it could be accessible to blind persons via an audio input. However, it would still be more complex for the voter than current systems, and voters would need to trust that the attached unit was secure.

Modular Voting Architecture. A third way to provide voter verifiability with DREs is analogous to optical scan or punchcard balloting with precinct counting.[110] After a voter makes choices on the voter interface (such as a touchscreen), the machine writes the ballot to a memory card or other device, called a *frog,* which the voter then takes to another machine that reads the ballot. This reader would be highly secure, as discussed above.[111] It would have a display so that the voter could verify choices before casting the ballot. A reader could even be

---

[107] For example, while a blind voter could use audio features of the DRE to make ballot choices, the voter could not verify those selections with a paper ballot unless it were printed in Braille. But most blind people do not read Braille (Braille Institute, "Braille Institute Services," 10 October 2003, [http://www.brailleinstitute.org/about-edu.html]), and Braille ballots would not provide complete ballot secrecy, since only blind people who read Braille would use them. A separate audio or other paperless verification device could, however, be provided. The U.S. Department of Justice has issued an opinion that DREs that produce voter-verifiable paper ballots are consistent with both HAVA and the Americans with Disabilities Act (P.L. 101-336) "so long as the voting system provides a similar opportunity for sight-impaired voters to verify their ballots before those ballots are finally cast" (Sheldon Bradshaw, Deputy Assistant Attorney General, "Whether Certain Direct Recording Electronic Voting Systems Comply with the Help America Vote Act and the Americans with Disabilities Act," Memorandum Opinion for the Principal Deputy Assistant Attorney General, Civil Rights Division, U.S. Department of Justice, 10 October 2003, available at [http://www.usdoj.gov/olc/drevotingsystems.htm]).

[108] For example, it would arguably be unlikely to deter certain forms of tampering, such as those that would not trigger a recount — for example, changing the vote by a small percentage in precincts where the vote was not close — and it does not take into account the vulnerabilities of printed ballots to various forms of election fraud.

[109] This is likely to be especially true for ballots on which the choices the voter made are printed. There would be no ambiguous marks or hanging chad for a machine to misread.

[110] See Caltech/MIT study, p. 58-64.

[111] See page 27.

provided with an audio program to allow blind voters to verify choices.[112] The advantages and disadvantages of this system are similar to those for the previous two, depending on its particular design.

Encrypted Votes. All three of the above approaches essentially provide a second, independent audit channel for the voting system. Another way of providing verifiability uses cryptographic methods to provide a kind of electronic verification.[113] Proponents argue that a properly designed system using encrypted votes is conceptually different from the "electronic ballot box" exemplified by DRE technology and that it provides for privacy, transparency, auditability, and security in a superior way to any current approach. This can be part of a more comprehensive system that uses cryptographic methods throughout the election process — from election preparation through auditing of the results — that purports essentially to mimic electronically or even improve upon the observability and transparency associated historically with manually counted paper ballot systems.

There are several different possible approaches using cryptographic protocols.[114] In one kind of system, the voter, before casting the vote in the voting booth, can see the ballot choices the encrypted information will correspond to. When the vote is cast, a receipt is generated with encrypted information, which could be in any of several different forms, such as a number or a pattern printed on a piece of paper.[115] After the election, each voter can also determine if his or her vote was counted as cast by comparing the receipt to posted information.[116] However, because the information on the receipt is encrypted, no one, including the voter, can prove what choices were made.[117] The encryption is performed with a set of encryption keys that have been generated independently by different election trustees — for example, an election

---

[112] However, this might better be done by a third, intermediary unit to keep the computer code in the reader as simple as possible.

[113] One application is described in VoteHere, "VHTi," 25 September 2003, [http://www.votehere.net/products_tech.htm].

[114] See, for example, Burmeister and Magdos, "Towards Secure E-Elections," p. 68-71. Most approaches appear to be based on one or both of two cryptographic protocols, asymmetric cryptography and homomorphic encryption (Danilo Bruschi and others, "E-Vote and PKI's: A Need, a Bliss or a Curse?" in Gritzalis, *Secure Electronic Voting*, p. 195-209).

[115] For example, the choices could be printed in plain text on the receipt and, when the voter casts the vote, be partially overprinted in a way that makes the text unreadable but retains characteristics that the voter can use to check later to see if the vote was counted as cast (David Chaum, "Secret-Ballot Receipts and Transparent Integrity," unpublished manuscript, May 2002). Alternatively, numeric codes on the receipt can be checked against those in a codebook in the voting booth (VoteHere, "VHTi," 25 September 2003, [http://www.votehere.net/products_tech.htm]).

[116] This provides voter verifiability.

[117] This seemingly paradoxical situation is possible through use of a cryptographic protocol known as a zero-knowledge proof, with which it is possible for one party to prove to another, with a very high degree of confidence (although not absolutely in the mathematical sense), that it possesses a particular piece of information, without revealing the information itself (Burmeister and Magdos, "Towards Secure E-Elections," p. 72).

administrator and representatives of each of the major political parties. Votes, to be counted, must be decrypted, which is accomplished by each trustee applying his or her key, and shuffling the votes before sending them to the next trustee.[118] Information related to the encryption is also posted that makes it possible for a trustee or a member of the public to audit and authenticate the election.[119] If a trustee (or anyone else) attempts to change, omit, or add any ballot, that will be detected in the audit, because the changes will show up as invalid, just as someone trying to modify an encrypted financial transaction will be discovered. At least one proposed system also permits auditing by observers during the course of the election.

Proponents of this approach claim that the capabilities of checking the vote before and after casting the ballot while maintaining ballot secrecy, along with the high probability of detecting any tampering through public auditing, means that, unlike with DREs, it is not necessary for voters or election or party officials to trust the voting machines to produce the correct tallies. In this sense, the encrypted-vote system is even more transparent than paper ballots that are hand-counted in the presence of observers. It is much closer in transparency to a roll-call vote, but it retains ballot secrecy. Proponents also believe that use of this approach could reduce the costs of elections by reducing the need for physical security, testing, and other activities. They also state that the integrity of the system is not dependent on the secrecy of the encryption keys, although privacy might be compromised if all keys were broken or stolen or all trustees colluded.

If successful, the approach could address many of the security issues with DREs that this report discusses. However, it does not yet appear to have been independently evaluated and therefore could have currently unknown disadvantages and vulnerabilities. Also, it is not clear that it would have the same potential positive impact on voter confidence as paper-based voter verification might. That is because a voter who does not understand the technology behind the system — and few voters are likely to — may have no greater basis for confidence in the correspondence between the encrypted receipt and the choices the voter made than is currently the case with DREs. Some proponents, however, believe that those concepts are simple enough that they can be taught in secondary school.[120]

If the system relies on printers at each voting booth, that raises issues similar to those with respect to printers for voter-verifiable paper ballots. Similarly, the verifiability feature increases the complexity of the voting process for voters, with unknown consequences. In addition, it is not clear to what extent valid ballots could be recovered in the event that tampering was found or malfunction occurred. Finally, some critics question whether encrypted receipts are in fact unable to show a voter's choices. Proponents argue that these concerns are either unlikely to be a problem in practice or are relatively easy to address.

---

[118] This is called a *mix-net* approach (Ibid., p. 68).

[119] This provides results verifiability.

[120] David Chaum, telephone conversation with author, 14 October 2003.

Options That Might Be Considered

The several methods proposed to address the verifiability issue — ranging from printing paper ballots to new electronic ways of voting — each have different strengths and weaknesses, making it difficult to determine at present whether any of these approaches should be adopted. At the same time, many observers would agree that finding ways to increase the verifiability and transparency of electronic voting is desirable. DRE technology is clearly evolving fairly rapidly and has not yet become settled, as witnessed by the diversity of available devices and features in comparison to other kinds of voting systems.[121] This environment may promote developing improved security and other desirable properties of the technology. At the same time, as jurisdictions continue to adopt DREs in response to HAVA and other factors, pressures to resolve security issues quickly may increase.

While a defense-in-depth approach would appear to be generally desirable for addressing security questions with DREs, as discussed above, any attempt to implement such an approach needs to take into account potential problems that can be associated with making substantial changes in the way an election is administered. For example, when a voting system is replaced in a jurisdiction, the proportion of residual votes and problems administering the election may actually increase initially, at least in part because neither voters nor pollworkers are familiar with the new system. In addition, there are no proven cases of tampering with DREs or other computer-assisted voting systems in public elections.[122] For these and other reasons, some observers argue that any changes to current technology and procedures should be incremental. Others, however, state that given the evolving threat environment and the concerns that have been identified, an incremental approach is not sufficient to prevent undetected tampering that could change the outcome of an election. Policymakers will need to weigh such differences in determining what if any actions to take in response to this set of issues.

Three general approaches are discussed below for addressing the issues raised in this report. First, action could be left to state and local jurisdictions that administer elections. Second, the EAC could address the issues. Third, Congress could take any

---

[121] As with many unsettled technologies, some problems have accompanied the evolution of this technology. For example, the Caltech/MIT study found that jurisdiction using DREs had a surprisingly large rate of *residual votes* (overvotes, undervotes, and spoiled ballots). There have also been reports of some problems encountered in jurisdictions recently acquiring the technology (see for example Kim Zetter, "Did E-Vote Firm Patch Election?" *Wired News,* 13 October 2003, [http://www.wired.com/news/politics/0,1283,60563,00.html]).

[122] According to a recent report, "the incidence of election fraud in the United States is low and...has had a minimal impact on electoral outcomes" (Lori Minnite and David Callahan, "Securing the Vote: An Analysis of Election Fraud," Dēmos, 2003, [http://www.demos-usa.org/demos/pubs/Securing_The_Vote.pdf]). However, there are documented cases of problems with DREs and other computer-assisted voting technology that have resulted in votes being lost, at least temporarily. For a compilation of cases, with sources, see Harris, *Black Box Voting,* p. 16–55. It could not be determined to what extent such problems go unreported, whether the options discussed in this report would reduce them, or if other kinds of voting systems would exhibit fewer problems.

of several possible actions. These approaches and options, which are not mutually exclusive, are discussed in turn below.

States. Elections are administered by state and local governments, with the federal government playing a circumscribed role. Although that role was substantially enhanced with the enactment of HAVA, the law stipulates that methods of implementation of its requirements are to be left to the discretion of the states (Sec. 305). States may therefore address these issues individually, as, for example, California, Maryland, and Ohio have already been doing.[123] The availability of federal funding under HAVA to improve election administration by state and local governments, as well as the creation of an independent federal agency whose purpose is to assist those governments in election administration, should improve the ability of those governments to ensure the security of elections. Leaving action to the states would allow them to react to the issues in a timely fashion and in ways that are most responsive to their individual circumstances and could lead to a variety of options being tested by different states, making it easier to determine which approaches work best. However, this approach might also lead to a patchwork of responses, which could be challenging for vendors to meet and could lead to some states being more vulnerable to tampering than others.

EAC. The Election Assistance Commission created by HAVA will have some responsibilities to provide guidance and to perform studies and research specifically relating to the security of voting systems. Its work in this area will involve NIST and others with experience in computer security. The EAC and its supporting boards and committees may provide an effective venue for addressing fundamental questions regarding voting system security and helping states meet their needs and responsibilities in this regard as well as issues relating to voter confidence in the security of DREs. One option would be that the EAC could perform an independent security review of current DREs. This might be especially useful if it could be done in cooperation with a selection of states exhibiting a range of security policies and procedures. However, to address the issue, the EAC must first form the relevant boards and committees, and any study would require a significant amount of time to complete. The EAC may not, therefore, be able to resolve the controversy before states need to make decisions about which kinds of voting systems to acquire.

Congress. Among the possible actions that Congress might consider are hearings, funding to address the controversy, and revisions to HAVA. Congress could choose to hold hearings on the issue for several purposes, such as clarifying issues and options, providing guidance to the EAC, or exploring funding and legislative options. It could also use other means, such as legislative report language or direct communication from congressional leaders, to encourage the EAC to address the controversy in an expedited manner.

Given the range of proposals for addressing DRE security issues, and the uncertainties associated with those proposals, Congress might also consider supporting research and development (R&D) in this area to identify the most appropriate solutions. In the past, economic incentives for private investment in such

---

[123] See discussion on pages 8–10 and elsewhere.

R&D have been weak, given the small, fragmented nature of the market for voting systems and the relatively low demand for sophisticated security for those systems. With the funding for new voting systems that HAVA provides, the evolving threat environment, and other factors, that situation may be changing. HAVA also authorized grants for R&D to improve security and other aspects of voting technology (Sec. 271), but Congress has not appropriated funds specifically for that program. Presumably, the EAC could use some of its general operating funds for such work, or Congress could appropriate funds specifically for it.

Several options for revising HAVA might be considered for a legislative response to the controversy:[124]

- A specific security provision could be added to the voting system requirements, stipulating, for example, that voting systems must adhere to security requirements for federal computer systems as required under current law,[125] or requirements or a mechanism to develop them that is specified in the provision.
- The voting system audit requirement in the Act could be revised to require a voter-verifiable paper ballot[126] or some other system of voter verifiability.
- Voting systems could be required to use open-source software.
- The Act could specify a security review and certification process for all voting systems.
- The Act could specify that experts in security be represented on the Technical Guidelines Development Committee.
- The EAC could be directed to provide security consultation services to state and local jurisdictions.
- The deadlines for meeting relevant requirements, such as for accessibility of voting systems, could be delayed pending resolution of the controversy.
- Federal funding could be provided for upgrades or replacements for DREs purchased under HAVA if they are shown subsequently to have significant security defects.

Some of the above options would themselves be controversial, as discussed earlier in this report with respect to voter verifiability and use of open source software. In addition, creating additional requirements would further increase the

---

[124] These are provided for information purposes only. CRS does not take positions on or advocate legislative and policy proposals.

[125] Relevant laws include the Computer Security Act (P.L. 100-235), the Paperwork Reduction Act (P.L. 104-13), the Clinger-Cohen Act (P.L. 104-106), and the Federal Information Security Management Act (P.L. 107-296).

[126] H.R. 2239 (Holt), the Voter Confidence and Increased Accessibility Act of 2003, includes this requirement, with a separate paperless system available for voters with disabilities. It would also requires "manual mandatory surprise recounts" in 0.5% of election jurisdictions, require the use of open-source software in voting machines, prohibit the use of wireless communications by voting systems, and require that all voting system hardware and software be certified by accredited laboratories.

federal role in election administration, which may be opposed by those who believe that it should be left to the states as much as possible. Options that would strengthen the ability of the EAC to help address this controversy may themselves be less controversial but might not lead to a timely resolution of the issues. Delays in meeting HAVA requirements are also likely to be controversial, and, some would argue, may not be necessary if the controversy can be resolved before 2006. Finally, additional funding authorization and appropriations may be difficult to enact in a constrained budget environment.

Conclusions

The purpose of this report has been to explain the controversy about the security of DREs and to lay out the issues raised and options for addressing them. The report does not attempt to resolve the controversy. However, some conclusions can be drawn with respect to the questions asked at the beginning of the report.

- Do DREs exhibit genuine security vulnerabilities? If so, could those vulnerabilities be exploited to influence an election?

Given the worsening threat environment for information technology and the findings of several studies and analyses discussed in this report, at least some current DREs clearly exhibit security vulnerabilities. Those vulnerabilities pose potential but not demonstrated risks to the integrity of elections, in that no proven cases exist involving tampering with DREs. Observers differ in their views about whether these potential risks are significant enough that they need to be addressed urgently or whether they can be addressed incrementally.

- To what extent do current election administration procedures and other security measures protect against threats to and vulnerabilities of DRE systems?

The answer to this question is a central point of contention in the controversy, with vendors and election administrators generally claiming that current measures are sufficient and certain other experts, most notably many computer scientists, and some activists claiming that they are not. These differences of opinion appear to be based in part on differences in philosophical perspective. Proponents of approaches such as voter verifiability believe that elections should rely for security on openness, transparency, and observability of the entire election process, and that currently too much trust is placed in the behavior and capabilities of vendors, election officials, and other involved parties. Many election administrators and vendors, and some other observers, believe that the views of such proponents are based on misunderstandings of how voting systems work and how elections are administered. They also believe that approaches such as a voter-verifiable paper ballot would not be of net benefit to the proper functioning of elections. Resolution of such fundamental differences may require — if it is in fact achievable — that those on both sides of this controversy develop better understanding of the bases for the views of the other side. Finding an effective solution may be easier if concerned computer scientists understand in detail how elections are run (perhaps by working directly

with administrators) and if election administrators understand cybersecurity more clearly (perhaps by working with computer scientists).

In any case, as indicated by some of the studies discussed in this report, significant improvements in the security of DREs may be found through careful analysis of current systems and how they are implemented and administered, without requiring voter verifiability or other substantial changes. However, such improvements in current systems are not likely to address the fundamental concerns raised by proponents of voter verifiability.

- Do those threats and vulnerabilities apply to computer-assisted voting systems other than DREs?

The potential threats and vulnerabilities associated with DREs are substantially greater than those associated with punchcard or optical scan readers, both because DREs are more complex and because they have no independent records of the votes cast. However, document-ballot readers are potentially subject to malware that could affect the count, to vulnerabilities associated with connection to other computers, and some other kinds of tampering. Therefore, the security of systems using readers might also benefit from some of the same kinds of approaches that have been proposed for DREs, such as improvements to current security policies and procedures, use of modern software engineering techniques, and use of strong cryptographic protocols.

- What are the options for addressing any threats and vulnerabilities that do exist, and what are the relative strengths and weaknesses of the different options?

The report discusses seven proposals for addressing the security issues raised about DREs. They include using current procedures and security mechanisms, with improvements as necessary; improving standards for the development and certification of voting systems; using open-source software for voting systems; and several methods to improve the transparency and verifiability of elections, including voter-verified paper ballots and an electronic version of that approach, use of modular electronic voting architecture that physically separates the voter interface from the casting and counting functions; and a system that uses cryptographic protocols to permit voters to verify that their ballots were cast as intended and that no votes were improperly changed, omitted, or added. These proposals vary in ease of implementation, the degree to which they have been tested in application, and the level of contention about both their ability to resolve the controversy and their overall desirability.

Most of the public debate has centered around whether to rely on current procedures and mechanisms or adopt voter-verifiable paper ballots. However, these are clearly not the only options, and the debate might benefit from fuller consideration of other possibilities such as those discussed above. In addition, several of the proposals discussed are not mutually exclusive, and a resolution of the controversy may involve elements of several proposals.

Three policy approaches, which are also not mutually exclusive, were discussed. The matter could be left to state and local governments, which administer elections; some states have already taken action. The newly formed EAC could address the issues through its convening power and responsibilities in the development of voluntary guidelines for and certification of voting systems. Congress could decide to use hearings or other mechanisms to provide guidance on the issues, or it might decide that a legislative solution is necessary. Several legislative options exist, ranging from funding for research on the issue to adding requirements on DRE security to HAVA. The benefits and disadvantages of these approaches depend on many factors, and a legislative solution may become more attractive if the controversy cannot be resolved through other means.

Ohio Secretary of State

Ohio Secretary of State
DRE Security Assessment

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

21 November 2003

InfoSENTRY Services, Inc.
www.infosentry.com
919.838.8570

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

192

Table of Contents

TABLE OF CONTENTS 2

INTRODUCTION AND BACKGROUND 3

PREVIOUS OHIO VOTING SYSTEM VENDOR EVALUATION 4
RESEARCH METHODS 5

SUMMARY OF SOURCE CODE FINDINGS AND RECOMMENDATIONS 10

PLANS, POLICIES, PROCEDURES: FINDINGS AND RECOMMENDATIONS 12

FINDINGS AND RECOMMENDATIONS FOR THE SECRETARY OF STATE'S OFFICE 13
FINDINGS AND RECOMMENDATIONS FOR DIEBOLD ELECTION SYSTEMS 14
SUMMARY OF FINDINGS AND RECOMMENDATIONS FOR ES&S 16
SUMMARY OF FINDINGS AND RECOMMENDATIONS FOR HART INTERCIVIC 18
SUMMARY OF FINDINGS AND RECOMMENDATIONS FOR SEQUOIA VOTING SYSTEMS 20

GENERAL FINDINGS AND RECOMMENDATIONS 23

CONCLUSION 25

APPENDIX 1: PRINCIPLE HAVA SECURITY SECTIONS 26

APPENDIX 2: THE STATE OF OHIO'S "INFORMATION SECURITY FRAMEWORK" 46

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

Introduction and Background

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

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

Previous Ohio Voting System Vendor Evaluation

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

Conclusions

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

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

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

Recommendations

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

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

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

Voting Systems

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

Research Methods

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

- Requirements tested
- Test scenarios used
- Test results

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

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

Table 1.
Voting Systems Tested by Compuware

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

11. Copies of any security awareness program documentation for any company teams or groups directly involved in the design, development, sale, distribution, maintenance, and support of the voting systems.

12. A copy of the most recent security audit(s) and management response(s) to the audit's findings for all information systems and organizations involved directly in the design, development, sale, distribution, maintenance, and support of the voting systems.

13. A copy of the most recent risk assessment(s) for all business processes and information systems involved directly in the design, development, sale, distribution, maintenance, and support of the voting systems, if the risk assessment material is not contained in and identified clearly in the information system security plan.

14. A copy of the current disaster recovery or business continuity plan for all business processes and information systems involved in the design, development, sale, distribution, maintenance, and support of the voting systems.

15. A copy of the results of the disaster recovery or business continuity plan test(s) for all business processes and information systems involved in the design, development, sale, distribution, maintenance, and support of the voting systems.

16. A copy of the most recent notification of ISO 9000 family of certifications for all organizations and business processes directly involved in the design, development, sale, distribution, maintenance, and support of the voting systems. (It will be helpful to receive also the date of initial certification(s)).

17. A copy of any notification of BS7799 or ISO17799 security certification for all systems involved in the design, development, sale, distribution, maintenance, and support of the voting systems.

18. A copy of technical documentation of (a) current voting system capabilities to provide a voter verifiable paper audit trail and (b) detailed plans for the voting system capabilities to provide a voter verifiable paper audit trail.

19. Copies of user documentation available from the vendor to the Ohio Secretary of State's office or Ohio's counties instructing them on operating and maintaining the voting systems.

20. A copy of the vendors' internal test plan(s) for **(a)** the voting systems proposed to the State of Ohio and **(b)** the voting systems that are currently moving through the certification process according to the 2002 Federal voting system standards (if those systems are not the same).

21. A copy of the test scripts and their results for the voting systems that relate to the security functions and capabilities of the systems in 20(a) and 20(b) above.

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

Summary of Source Code Findings and Recommendations

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

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

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

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

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

Plans, Policies, Procedures: Findings and Recommendations

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

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

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

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

Findings and Recommendations for the Secretary of State's Office

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

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

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

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

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

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

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

Findings and Recommendations for Diebold Election Systems

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

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

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

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

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

Summary of Findings and Recommendations for ES&S

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

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

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

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

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

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

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

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

Summary of Findings and Recommendations for Hart InterCivic

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

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

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

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

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

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

Summary of Findings and Recommendations for Sequoia Voting Systems

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

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

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

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

General Findings and Recommendations

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

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

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

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

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

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

Conclusion

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

Appendix 1: Principle HAVA Security Sections

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

SEC. 221. TECHNICAL GUIDELINES DEVELOPMENT COMMITTEE.

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

(b) Duties.--

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

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

(c) Membership.--

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

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

(i) Members of the Standards Board.

(ii) Members of the Board of Advisors.

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

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

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

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

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

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

(B) methods to detect and prevent fraud;

(C) the protection of voter privacy;

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

SEC. 241. PERIODIC STUDIES OF ELECTION ADMINISTRATION ISSUES.

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

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

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

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

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

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

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

(2) Ballot designs for elections for Federal office.

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

(4) Methods of conducting provisional voting.

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

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

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

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

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

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

(A) a legal public holiday under section 6103 of

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

(a) Study.--

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

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

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

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

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

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

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

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

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

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

(a) Study.--

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

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

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

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

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

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

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

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

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

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

(I) the impact of technology on the speed,

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

(b) Report.--

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

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

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

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

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

(d) Recommendation of Topics for Research.--

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

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

SEC. 302. PROVISIONAL VOTING AND VOTING INFORMATION REQUIREMENTS.

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

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

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

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

(B) eligible to vote in that election.

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

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

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

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

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

(b) Voting Information Requirements.--

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

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

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

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

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

(1) Implementation.--

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

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

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

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

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

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

elections for Federal office.

(2) Computerized list maintenance.--

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

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

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

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

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

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

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

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

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

(5) Verification of voter registration information.--

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

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

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

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

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

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

(B) Requirements for state officials.--

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

registration.

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

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

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

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

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

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

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

"(D) For purposes of this paragraph--

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

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

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

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

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

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

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

(2) Requirements.--

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

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

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

that shows the name and address of the voter.

(B) Fail-safe voting.--

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

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

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

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

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

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

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

(I) a driver's license number; or

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

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

(C) who is--

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

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

States.

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

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

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

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

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

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

(d) Effective Date.--

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

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

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

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

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

This document contains CONFIDENTIAL and PROPRIETARY information. It is not for distribution without the express consent and permission of the Ohio Secretary of State.

Dean Heller
Nevada Secretary of State

News Release
December 10, 2003

Secretary of State Heller Announces Direct Recording Electronic Voting Machine Choice

Heller mandates Nevada become first state to require voter verifiable receipt for 2004 election

---

Carson City -- Secretary of State Dean Heller announced at news conferences today in Reno and Las Vegas his decision to purchase for all Nevada counties Direct Recording Electronic (DRE) voting machines. In an unprecedented move, he also announced he is mandating a voter verifiable receipt printer be included on all newly purchased DRE machines for the 2004 election. In doing so, Heller becomes the first state election official to demand a voter verifiable receipt before the 2006 election. He added that all existing machines statewide must add the printer technology by 2006. Heller also read a proclamation decertifying all punch-card voting machines in Nevada as of September 1, 2004.

"Voting is the most fundamental freedom Americans enjoy; it is the backbone of a free and democratic society," Heller said. "As the State's Chief Elections Officer, my duty is clear: to provide voters with the highest level of confidence that elections in this state are fair, unbiased and secure. These critical principles led to my decision to be the first state in the nation to demand a vendor to include a voter verifiable receipt (VVR) printer on all DRE machines in time for the 2004 election. It is a right of every citizen to feel secure that the voting choices they have made are recorded accurately. A paper trail is an intrinsic component of voter confidence."

Senator John Ensign, whom Heller has spoken with several times over the VVR issue, added, "I have been a strong and vocal advocate for approval of federal legislation requiring paper verification of ballots. As public officials, we have a serious responsibility to maintain the integrity of our election process, including voting machines and ballots."

"Throughout the process of selecting a vendor and making the determination to eliminate punch-card machines, I relied on three criteria: which voting equipment is the most accurate, most secure and has the highest degree of voter confidence," Heller stated. "Sequoia Voting Systems DRE machines met these essential demands. The Florida debacle and the chaos created by the 'hanging and pregnant chad' controversy clearly demonstrate the need to move forward with advanced technology. DRE machines provide a greater ability to accurately record the will of the people."

"As we moved through this process, several factors helped make my decision clear," Heller said. "Foremost were the findings of a report I requested from the Nevada Gaming Control Board to review

the two systems preferred by the overwhelming majority of state County Clerks/Registrars of Voters: Sequoia and Diebold." The report, compiled by Electronic Services Division Chief Marc McDermott, stated in its summary:

> *I believe the Diebold electronic voting machine, operating on the software analyzed in a John Hopkins report and the SAIC (Science Applications International Corporation) Risk Assessment Report, represents a legitimate threat to the integrity of the election process. Conversely, based on available information with regard to the Sequoia Voting System, I believe the Sequoia electronic voting machine represents a much more secure option because of the increased security of the customer (voter) interface and by the fact that the Sequoia operating software has not been made available on the Internet.*

When the **Gaming Control Board's Electronic Services Division reports** to me that one system is superior to another, I'm going to place my confidence in that equipment," Heller said. "They are responsible for verifying the security and integrity of various electronic gaming machines throughout Nevada and, therefore, accountable for millions of dollars on a daily basis. My level of confidence in selecting Sequoia was greatly increased after receiving this report."

Heller said there were several other factors in his decision to select Sequoia Voting Systems for the entire state, including the fact that 70% of the state's voters already utilize Sequoia DRE voting machines. "Clark County has successfully used Sequoia DRE's for the past 10 years," Heller said. "That means the majority of Nevada voters are already comfortable and experienced in using this style of DRE machine." DRE's have several advantages to other voting equipment:

- Voter's ability to review and correct ballot choices onscreen
- Chad-free election
- User-friendly technology voters encounter every day
- Reduction in number of residual (over/under) votes
- Improved voting experience
- Larger font types for voters who have vision problems
- Allows visually impaired and other disabled voters greater access and ease of use
- Able to be programmed with multiple languages
- Rapid tabulation and reporting of vote totals

Another factor was a vote by the state's County Clerks/Registrars of Voters during the County Fiscal Officers Association meeting in Yerington on June 19, 2003, in which, after three vendors-Sequoia, Diebold and ES&S-gave presentations, the Clerks/Registrars preferred Sequoia's DRE machine by a 12-3 (with one "no preference") vote.

Heller also restated his reasons for going with one vendor for all machines statewide: "That choice was made for several reasons, including the fact that every voter at polling places in Nevada on Election Day will now be using the same voting system and technology. It will also allow for a smoother transition to a statewide voter registration system, which Nevada must complete and have operational before the 2006 election to meet a requirement mandated by Congress through the Help America Vote Act. Furthermore, cross training of poll workers and Information Technology personnel, along with the ability for counties to borrow equipment from each other in a crunch, were further compelling reasons for me to believe the decision to go with one vendor was in the best interest of all Nevada voters."

The voter verifiable receipt allows voters to see their ballot choices on a written receipt under glass before finalizing their vote. Currently, Clark County's Sequoia DRE's do not include a voter verifiable

receipt (VVR). Many election officers and officials across the nation and in Nevada have stated they do not feel the VVR component is necessary. But Heller said voter confidence is critical to the integrity of the voting process. "By requiring a VVR printer to be a component of each DRE machine, voters will be confident their choices are being recorded accurately," Heller stated

"Although cost should always be a factor when an elected official is determining how to spend taxpayer money, when it comes to how we exercise the most fundamental freedom Americans enjoy, money takes a backseat to accuracy, security and voter confidence," Heller said. "Regardless of the additional cost of adding VVR printers, in my mind, it is clearly the right thing to do. My conclusion is overwhelmingly supported by Nevadans, based on the comments I have heard from our citizens via phone calls, emails, letters and town meetings."

The VVR printer is attached to the DRE terminal. After a voter makes his or her choices for various offices and ballot questions, the machine will print a copy of the selections that appears under a glass case. If the voter agrees with the printed receipt, he or she is prompted to cast their permanent ballot. If the voter disagrees with the information on the paper receipt or wishes to change their selections, the voter can reject the VVR and go through the selection process once again. The voter is not able to physically touch the receipt at any time during the voting process. When the voter's choices are finalized, the receipt is forwarded on the recording spool so that no one can see any other person's voting choices. The receipts would be used if a recount were ordered.

As the State's Chief Elections Officer, Heller took the additional step of officially decertifying all punch-card voting machines in Nevada. Currently, seven counties-Carson, Churchill, Douglas, Humboldt, Lincoln, Lyon and Storey-utilize punch-card machines for voting. Clark County uses punch-card machines for absentee voting only.

Funding to buy the Sequoia DRE machines and the VVR printers will come from federal money allotted to the states through the passage of The Help America Vote Act (HAVA), which was signed into law by President George W. Bush on October 29, 2002. Under Title I of the Act, Nevada received the minimum state allotment of $5 million. The State is scheduled to receive an additional $15 million under the provisions of Title II of the Act.

SOS Contact Information

SOS Home | Legislature | Nevada Home

Copyright © 1996-2003
Page last updated on 12/10/2003

Secretary of State's

Ad Hoc Touch Screen Task Force

Report

SECRETARY OF STATE KEVIN SHELLEY

July 1, 2003

TABLE OF CONTENTS

Introduction 2

Executive Summary 4

Background And Overview 15

Major Issues And Questions Addressed By The Task Force 18

1. Computer Security 18
2. Administrative Security 19
3. Voter Confidence 21
4. Voter Verification 21

Legal, Technical, And Procedural Constraints 24

1. Federal And State Laws: Accessibility For The Visually Impaired, No/Low Literacy Voters And Non-English Speakers 24
2. Court Ordered Conversion 25
3. Product Development And Testing Challenges 26
4. Disaster Avoidance 26
5. Voter Issues 27
6. Election Administration 27
7. Printer Issues 27
8. Marketplace 28
9. Reimbursement 28

Recommendations 30

1. Security 30
2. Printing a Permanent Paper Record 33
3. Voter Verified Paper Audit Trail 38
4. Alternative Verification Methods 42

Conclusions And Next Steps 47

Appendix: Glossary of Terms 49

Submittal 54

INTRODUCTION

Secretary of State Kevin Shelley created the Ad Hoc Touch Screen Task Force on February 19, 2003 in response to concerns expressed over the security of DRE voting equipment. The purpose of the Task Force was to study these concerns, discuss possible improvements, and to make recommendations to the Secretary of State and the Voting Systems and Procedures Panel.

The Task Force is comprised of individuals who brought vastly different backgrounds, experience, and views on these issues. Over the course of eight meetings, the Task Force heard from the Secretary of State, local election officials, voting system vendors, experts in computer security, a representative of an independent testing authority, a representative of the NASED ITA Technical Subcommittee of the Voting Systems Board, and representatives of the disabled and civil rights community.

This report represents a consensus view on the issue. However, with such diverse backgrounds and such a limited time to provide recommendations, it is clear that this committee has not made recommendations on every aspect of this issue. As such, we have provided a range of options with an explanation for each.

The Task Force is comprised of the following individuals:

Mark Kyle, Undersecretary of State (Chair)
Marc Carrel, Assistant Secretary of State for Policy & Planning (Co-Chair)
Kim Alexander, Founder and President of the California Voter Foundation
David Dill, Professor of Computer Science, Stanford University
David Jefferson, Computer Scientist, Lawrence Livermore National Laboratory
Robert Naegele, President, Granite Creek Technology, Inc.
Shawn Casey O'Brien, former Executive Director, Unique People's Voting Project
Mischelle Townsend, Registrar of Voters, Riverside County

Charlie Wallis, Department IT Coordinator, San Diego County Registrar's Office
Jim Wisley, Office of Assembly Speaker Herb Wesson

In addition, the members of the committee would like to thank the efforts of John Mott-Smith, Dawn Mehlhaff, Bruce McDannold, Debbie Parsons, and Terri Carbaugh of the Secretary of State's Office, and InfoGard Laboratories for their assistance to the Task Force.

EXECUTIVE SUMMARY

Secretary of State Kevin Shelley created the Ad Hoc Touch Screen Task Force on February 19, 2003 in response to concerns expressed over the security of Direct Recording Electronic (DRE) voting equipment. The purpose of the Task Force was to study these concerns, discuss possible improvements, and to make recommendations to the Secretary of State and the Voting Systems and Procedures Panel.

In March of 2002 California voters enacted the Voting Modernization Bond Act, establishing a fund of $200 million for counties to upgrade their voting equipment. In 2002 the federal government enacted the Help America Vote Act requiring election reform and providing funds to, among other things, have at least one voting machine in each polling place that is accessible to the blind and visually impaired. The same year, the State enacted AB 2525 (Jackson), Chapter 950, Statutes of 2002, requiring voting equipment be accessible to persons with visual disabilities when a county purchases new voting equipment.

These laws and a federal court order created an incentive for counties to purchase DRE voting equipment (which includes touch screen voting systems) and move away from paper ballots and earlier mechanical voting systems. This has led some members of the public to raise concerns regarding the security of the DRE systems. Essentially, the argument is that DRE voting equipment relies on a "black box" computer with proprietary source code and object code hidden from the public, and therefore the potential exists for unknown reliability and security risks.

The public discussion of the security of touch screen voting equipment has primarily focused on the issue of a "paper trail" or paper audit trail, and whether (and what type) would be necessary to back-up the electronic record of the vote. While there exists a paper audit trail requirement in state and federal law, some have advocated this be a "voter verified" paper record so voters can verify their choices on paper before their ballots are cast. Other audit methods have also been discussed.

These issues are at the core of what the Ad Hoc Touch Screen Task Force was constituted to address. The four key issues addressed by the Task Force were: (1) Computer Security: Whether there is evidence of a security issue with DRE voting systems and, if so, the nature and probability of the security issue ; (2) Administrative Security: Whether the existing federal, State and local tests are adequate, and whether current security protocols and processes used by DRE vendors are adequate; (3) Voter Confidence: How to ensure voter confidence in our voting systems and elections; and (4) Voter Verification: Whether verification by voters is useful or not; whether verification by voters is necessary or not?

After examining these questions, the Task Force examined the many legal, technical and procedural constraints which surround them. These include: (1) Federal and state laws involving the accessibility of the blind or visually impaired voters, voters with no or low literacy, and those who do not speak English; (2) The court ordered replacement of punch card voting systems in California; (3) Challenges affecting the development of new or improved products and the federal and state testing process required; (4) Efforts to create problems by imposing new mandates or burdens too quickly, which could detrimentally impact the 2004 elections; (5) Issues involving the administration of elections; (6) Issues related to printers; (6) The realities of the marketplace; and (7) The cost to implement any solution recommended and the requirement that such costs could be borne by the State.

FINDINGS

The following are the major findings of the Task Force:

- *Voting equipment should and must meet the requirements of federal and state laws requiring access to voting.*

- *The time requirements for product development and certification are significant issues in terms of the timing of the development of potential market solutions to address any of the issues brought up in this report.*

Concepto Principal

- *Any recommendations to change current voting equipment recognize the paramount importance of a successful election in terms of voter confidence, and no recommendations should be utilized to undermine the successful administration of those elections.*

- *Any proposed method of verification must not inconvenience voters, create lines at the polling place, or otherwise discourage voters from casting a ballot.*

- *Any new equipment options should be as simple to administer as possible so as to not create unnecessary complexity at the polling place.*

- *There are a number of logistical challenges that are present with any paper-based voting system using printers and these challenges need to be explored and understood in greater detail.*

- *Local jurisdictions, if they desire independent verification on their systems, should have a range of verification options to choose from, including paper-based and electronic options.*

- *State or federal funds should be provided to pay the cost of upgrading any system that does not meet the requirements implemented as a result of the recommendations of this report.*

- *Its recommendations should be considered with the understanding that California's testing and certification procedures are considered among the*

strongest in the nation, and DRE systems currently used in California are certified to conduct an accurate and reliable election.

RECOMMENDATIONS

Based on these findings and after hearing testimony from a wide range of experts, the Task Force agrees that there are four major areas deserving recommendations to the Secretary: Security, Paper Records, Voter Verification, and Independent Verification:

1. SECURITY

FEDERAL TESTING - There is general agreement on the Task Force that the federal testing standards and procedures should be substantially improved to enhance security and other aspects of voting equipment.

The Task Force offered nine recommendations to improve the federal testing process *(see pages 27-29)*. These include:

- Opening up the federal testing process to citizen observation.
- Altering the Federal testing and qualification process from a one-time testing process to an ongoing process involving periodic review.
- Making sure that all systems in use in California are retested under the most current federal standards.
- Charging the National Institute of Standards and Technology (NIST) with conducting ongoing oversight of the Independent Testing Authorities (ITAs)
- Providing federal funding to enable NIST to conduct ITA oversight and to increase the technical security of systems.
- Removing the blanket exemption for testing of Commercial Off-The-Shelf (COTS) software for systems without voter verification.

- Establishing a national database that is maintained at the federal level to track and document problems found in election systems in order to keep local jurisdictions and the public informed.

STATE TESTING- There is general agreement on the Task Force that the state process for certification and testing should be substantially improved to enhance the security and other aspects of voting equipment. The Task Force makes 13 recommendations to improve the State testing process *(see pages 29-31)*. These include:

- Assuring that all ITA and NIST activities have been successfully completed as a prerequisite to certification testing.
- Developing model Operational Security, Communications Security and Data Security procedures to be adopted for use by local jurisdictions.
- Requiring vendors to provide complete operating procedures in order to obtain certification.
- Altering the State certification process from a one-time testing process to an ongoing process involving periodic review.
- Creating a Technical Oversight Committee comprised of technical experts who can improve current testing and code-review standards, provide expert guidance throughout the certification process, and review software and hardware issues.
- Requiring a "threat analysis" from the federal ITA as part of all required documents before state testing of a vendor's system can begin.
- Ensuring that the software code approved at the state and federal levels is identical to the code used at the local level, by requiring the ITAs to provide the State with the executable code of each system to be tested and to develop a system to compare that code with what counties use on their machines.

- Obtaining copies of everything that each vendor provides to the federal testers, including source code, along with all the documents prepared during the Federal testing process. All of these documents, except the source code and the threat analysis, would be public documents unless the vendor could establish that a document meets certain public standards of confidentiality or proprietariness established by the State, enabling the document to be privileged.
- Conducting random audits of machines throughout the state to assure that software code held by the State is the same code in use on each machine.
- Conducting random on-site sampling (otherwise known as "parallel monitoring") of a specific number of machines on Election Day to confirm that each system in operation is registering votes accurately.
- Making voting system procedures easier for the public to find and access.

LOCAL TESTING AND PROCEDURES –There is general agreement on the Task Force that the process of acceptance testing can be improved to enhance the security of the process. There is also general agreement that Logic and Accuracy testing is essential for pre-election and post-election testing of voting equipment and provides substantial safeguards against error and machine malfunction, but these tests can also be improved. The Task Force makes three recommendations to improve the local testing process *(see page 32)*.

- Creating penalties for local jurisdictions that utilize systems that are not certified.
- Protecting systems from hackers by requiring local jurisdictions to be on an isolated network and to refrain from connecting voting machines to the Internet at any time.
- Preventing the system vendor from conducting the Logic and Accuracy tests on a voting system. ???

DISTRIBUTION OF SOFTWARE and TESTING – To ensure the security of systems when traveling between entities and to ensure that a voter has not missed a selection, the Task Force makes three recommendations in these areas *(see page 32)*.

- Distribution of qualified voting system software should be tightly controlled. NIST should distribute qualified object and source code to the State, and the State, not the vendors, should control the distribution of object code to the local jurisdiction using that system.
- Restricting voting system vendors from altering object code without retesting and re-certification.
- Requiring a review screen on all DRE systems in order to minimize unintentional "undervotes," which must also be included on any audio accessories available for those with visual disabilities, low literacy, and limited manual dexterity.

VENDOR SECURITY - In order to assure that the internal security systems are improved, the Task Force makes four recommendations *(see page 33)*.

- Requiring vendors to conduct background checks of programmers and developers using standards established by the State.
- Establishing strict internal security protocols and procedures for vendors to comply with during their software development process.
- Requiring vendors to document a clear chain of custody for the handling of software.
- Imposing civil liability and stiff criminal penalties if any malicious code is found before, during, or after certification, whether such malicious code interferes with an election or simply was intended to. The liability and

penalties must apply to the programmer or developer of the malicious code as well as to the vendor employing the individual(s).

2. PRINTING A PERMANENT PAPER RECORD

Both Proposition 41 and the federal Help America Vote Act of 2002 (HAVA), require a paper audit trail be prepared for each polling place. This is separate and apart from whether this paper audit trail is provided to the voter to verify his or her vote before their vote is cast.

The Task Force agrees that to provide this required permanent paper record, that each local jurisdiction not using a voter verified paper audit trail, print out each voter's ballot as a record of the vote shortly after the closing of the polls. This process should be open to viewing by the public. For technical and logistical reasons there is no support to have the printing of this permanent paper record done at the time the ballot is cast (unless the system allows the voter to verify his or her vote on paper). Each local jurisdiction should also provide per-precinct ballot images to the State, which should make them available to the public on CD-ROM.

The Task Force also agrees that on all DRE systems, the electronic vote should be the legally valid vote unless there is some sort of discrepancy between it and the permanent paper record. For the mandated 1% manual recount or in the case of a full recount, the paper record should be presumed to be more reliable than the electronic vote unless there is evidence it has been corrupted or is incomplete.

3. VOTER VERIFICATION

There was no consensus on the issue of whether a voter verified paper audit trail (VVPAT) should be required on all voting systems certified and used in California. However, the Task Force did agree that systems with a VVPAT should be an option for local jurisdictions to choose, if such systems can meet the disabled and language accessibility requirements of State and federal law.

In addition, for jurisdictions that choose to utilize systems with a VVPAT, the Task Force recommends that the state's certification advisory body, the Voting Systems and Procedures Panel, , review and address a series of issues related to VVPAT to ensure that all vendors utilizing such an option are conforming to consistent standards.

4. ALTERNATIVE VERIFICATION METHODS

Because of reservations about paper-based voter verification, the Task Force wanted to encourage the development of alternative voter verification technology, such as fully electronic verification, that would ensure the security of each vote as well as provide greater voter confidence. The Task Force suggests the State explore the development of such methods.

Because of the increased protections imposed by Election Day sampling, the Task Force agreed that there is time for vendors to develop alternative voter verified audit methods. But the Task Force agreed that there needs to be voter verification imposed by a date certain and the State and federal governments must provide funding to make this happen. There was disagreement, though over what type of voter verification audit mechanism to require, and on what timeline.

Six members of the Task Force would require an electronic verification method, but they feel it will take some time to perfect a version a federally qualified, state certified, and mass produced version that can be integrated into a DRE. As such, this group recommends the State allow vendors until December 31, 2006 to develop and obtain certification for such a solution, and at that point restrict vendors' ability to sell DRE systems without an electronic verification feature. All voting systems purchased prior to that date should be modified to include electronic verification by 2010.

Meanwhile, three Task Force members believe strongly that the state should impose a voter verification audit requirement immediately, and that no additional DRE voting equipment should be purchased unless it meets that requirement. This group is greatly

concerned about the number of new purchases of DRE systems that are scheduled to occur before 2007. If a voter verified audit trail requirement is not imposed immediately, this group feels that it is vital that any new purchases of DREs be planned and budgeted with the conversion to this requirement in mind. To achieve this, this group believes that the State should mandate a voter-verified audit trail requirement (either with alternative verification or a voter verified paper audit trail), by January 2007 for all equipment deployed from now on (this deadline could be extended until 2010 for DREs currently in use). In addition, the state should strongly encourage all counties moving to deploy DRE voting systems to implement the requirement as soon as possible in advance of the deadline.

Therefore, the Task Force members are not far apart on imposing verification for all DRE systems in California – 3 years – and not far apart on the types of verification - with all members encouraged by the possibility of electronic or alternative verification methods, but three members believing that paper –based voter verification should be required immediately until electronic or other alternative voter verification methods are feasible.

All members also agree that prior to state certification testing, conformance with the electronic independent audit requirements should be determined by the Voting Systems and Procedures Panel, in consultation with the Technical Oversight Committee mentioned above.

All the members also agreed that it is imperative that voter confidence in voting systems currently in use not be eroded by our efforts to add additional layers of security to the process.

CONCLUSIONS

The Task Force members urge the Secretary and others to consider these recommendations and, given the importance that accurate election results are to our

democracy, to seek their implementation at the local, state and federal levels. The Task Force recognizes the potential cost of implementing these recommendations, but urges the federal and state governments to make the necessary financial commitment.

BACKGROUND AND OVERVIEW

For the last 40 years, Californians have primarily voted on mechanical voting equipment using paper ballots that require the voter to either punch a hole in a card to indicate a vote selection, or to mark the ballot with a marking device. After the polls were closed, these ballots were collected from polling places and brought to a central location for counting.

The presidential election in Florida in 2000 focused attention on the weaknesses of paper ballots, including "chad" and the difficulty of establishing voter intent. The newspapers were full of pictures of election officials holding ballots up to the light to see if they could determine if the "pregnant chad" meant that the voter intended to punch a hole and cast a vote or not.

As a result of the difficulties experienced in that election, election professionals began examining the advantages of direct recording electronic (DRE) voting equipment (this category includes touch screens) and there was a movement away from using paper ballots. The advantages of DRE systems include: (1) no "chad"; (2) eliminating the possibility of an "overvote" (or making more selections than permissible) and advising the voter of any "undervote" (when a voter makes fewer than the maximum number of permissible selections in a contest); (3) providing persons who are blind, visually impaired or physically disabled with the opportunity to cast a secret ballot without assistance; (4) facilitating "early voting" and thereby encouraging greater voter participation; (5) eliminating marking devices which can result in questions of voter intent, and (6) providing a review screen before a voter casts a ballot.

In February of 2002 a federal judge ordered that all pre-scored punch card voting equipment in use in California be replaced not later than January 1, 2004. This order requires Alameda, Los Angeles, Mendocino, Sacramento, San Bernardino, San Diego, Santa Clara, Shasta, and Solano counties, home to 56% of the state's voters, to convert to new voting systems.

The election in Florida in 2002 illustrated additional problems, notably the difficulty of converting to a new voting system, and the potential to disenfranchise voters if poll workers are poorly trained in the operation of new voting equipment. Reports following this election indicate that one of the principal reasons for problems was the lack of smaller local elections prior to a major statewide election in which to work out any technical and procedural bugs in the new systems and to train poll workers and voters how to use the new equipment.

In March of 2002 California voters enacted the Voting Modernization Bond Act, establishing a fund of $200 million for counties to upgrade their voting equipment. This provided a strong incentive, and momentum, for even more counties, in addition to the nine counties required by the court order, to also convert to new voting systems.

In October of 2002 the federal government enacted the Help America Vote Act requiring election reform and providing funds to, among other things, have at least one voting machine in each polling place that is accessible to the blind and visually impaired.

Also in 2002, the California Legislature enacted AB 2525 (Jackson), Chapter 950, Statutes of 2002, requiring that voting equipment be made accessible to persons with visual disabilities when a county purchases new voting equipment with Voting Modernization Bond Act or Help America Vote Act funding.

As a result of these new laws, California and other states began to purchase and install DRE voting equipment. To date, Alameda County, Plumas County, and Riverside County have converted entirely to DRE voting equipment. Several other counties are either testing DRE equipment in "early voting" environments, using it for smaller city elections, or are in the middle of contract negotiations to purchase these systems.

As elections officials have moved away from the earlier mechanical voting systems, some members of the public have raised concerns regarding the security of the new

DRE systems. Essentially, the argument is that DRE voting equipment relies on a "black box" computer with proprietary source code and object code hidden from the public, and therefore the potential exists for unknown reliability and security risks such as insertion of malicious code by an insider at a voting equipment vendor to manipulate the software of these machines in a way that would not be detectable and could affect the outcome of one or many elections simultaneously.

The public discussion of the security of touch screen voting equipment has focused primarily on the question of what kind of "paper trail" or paper audit trail is necessary to back-up the electronic record of the vote. In particular, apart from an existing paper audit trail requirement in state and federal law, some have advocated a "voter verified" paper trail – a paper record of the voter's choices that the voter can use to verify his or her vote choices before casting their ballot or otherwise stored as a check against manipulation, fraud or error.

Although the public discussion has focused primarily on a voter verified paper trail as a means of further protecting against fraud or error, it is important to acknowledge that this protection can probably also be provided through an internal electronic audit mechanism. In addition, other procedural safeguards are available to increase detection of attempts to manipulate the accuracy or integrity of the voting system.

These potential security issues are the core of what the Ad Hoc Touch Screen Task Force was constituted to address, and the details of these issues are enumerated in the "Security Issues" section of this report below.

MAJOR ISSUES AND QUESTIONS ADDRESSED BY THE TASK FORCE

1. COMPUTER SECURITY

One question the Task Force addressed was: Is there evidence of a security issue with DRE voting systems and, if so, what is the nature and probability of the security issue?

The essential argument espoused by several computer scientists is that computerized voting equipment requires reliance on a "black box" and that it is possible that subtle program flaws can affect vote recording or "malicious code" can be added to software in that voting equipment in a way that is extremely difficult to detect. By way of example, this malicious code could be added by a "rogue programmer" and be timed to activate at a future election date to switch 1% of the votes across many jurisdictions for candidates of party A to the candidate of party B. Theoretically, malicious code could also be inserted by a voting system vendor conspiring to alter an election or by others.

The Task Force agrees that, in theory, there is a possibility of a security threat with DRE voting equipment. The Task Force, however, disagrees about the likelihood of the possibility that malicious code could be added to a voting system and be undetected by the federal, state, and local independent testing authorities. Some members (including the computer scientists on the Task Force) assert a high risk while others assert a very low probability.

But the Task Force agrees that there is no proven instance of such an attempt at fraud that has happened in the number of years that DRE voting equipment has been in use.

The Task Force further agrees that setting aside a number of touch screen voting systems on election day, equipment that was prepared exactly like all other equipment used by voters but which is instead voted by trained personnel, can increase the

likelihood of detection of attempts by "rogue programmers" or others to manipulate the software of a voting system. This Election Day sampling would be conducted under precise conditions to exactly replicate those at the polling place.

As the computer industry has evolved, there has been a corresponding evolution of "hackers" and others to disrupt or defraud computer systems. In response to this, there has also been the development of an industry to provide security to computer systems. This security industry, in assessing the risk to a given computer application, begins with a "Threat Analysis" to define the types of security attacks to which a computer system might be vulnerable. This is a complicated analysis and the Ad Hoc Touch Screen Task Force does not possess the expertise, time or the resources to conduct a definitive and professional "Threat Analysis" of the entire voting process, but it may be appropriate for this analysis to be commissioned, funded, and conducted by others.

2. ADMINISTRATIVE SECURITY

FEDERAL TESTING - All voting equipment and systems used in elections in California are required to be tested by the federal and state governments. Initial qualification testing is done by an "Independent Testing Authority" (ITA) and uses guidelines adopted by the federal government for voting system performance and security. Both the hardware and software of voting systems are analyzed and tested.

There is general agreement on the Task Force that the federal testing standards and procedures should be substantially improved to enhance security and other aspects of voting equipment.

STATE TESTING AND CERTIFICATION - Once voting equipment has received federal qualification, it is eligible to apply for certification by the state for use in California elections. This certification process requires further testing by an internationally renowned voting systems consultant on contract with the state. This consultant conducts performance tests to ensure that the equipment is accurate and secure and

can conduct elections according to California law. In addition, the applicant must demonstrate the equipment to election officials, interest groups (such as persons who are blind or visually impaired), and others. The applicant is currently required to place the source code that operates the voting system in an escrow facility and to produce an extensive manual of procedures for the use of the equipment. The voting system is considered for certification at a public meeting of the state's Voting Systems and Procedures Panel.

There is general agreement on the Task Force that the state process for certification and testing should be substantially improved to enhance the security and other aspects of voting equipment.

LOCAL TESTING AND PROCEDURES – Once a voting system is certified for use in California, local elections officials may purchase the system for use in their jurisdiction. Currently, there are several different technologies certified for use by the Secretary of State, including DRE systems, optical scan equipment (of multiple varieties), and punch cards (pre-scored punch cards will be decertified as of 2004). The choice of which voting system to use is made by each local jurisdiction (county or city).

When voting equipment is purchased, the local elections official is required to conduct "acceptance tests" on the equipment.

There is general agreement on the Task Force that the process of acceptance testing can be improved to enhance the security of the process.

At every election, all voting equipment is required to be tested by the local elections official conducting the election. This testing includes "Logic and Accuracy" testing, a process during which voting equipment is tested with a known number of votes and must produce exactly that result in order to be certified for use in the election. Once certified, it is sealed and if tampering occurs there are security procedures in place for the machine to be removed from service.

There is general agreement on the Task Force that Logic and Accuracy testing is essential for pre-election and post-election testing of voting equipment and provides substantial safeguards against error and machine malfunction. There is also general agreement that these tests can be improved.

3. VOTER CONFIDENCE

It is vitally important that all Californians have confidence in the integrity of the electoral process, including the equipment on which they cast their votes. Although the technology of voting is changing and becoming more and more computer based, all California voters should have confidence that elections officials and others are engaged in a process of continuous improvement to ensure that voting equipment keeps up with the challenges of new technology. The Task Force feels its recommendations should be considered with the understanding that California's testing and certification procedures are considered among the strongest in the nation, and DRE systems currently used in California are certified to conduct an accurate and reliable election.

4. VOTER VERIFICATION

The final issue examined by the Task Force is that of verification by the voter of his or her ballot.

The recently enacted federal Help America Vote Act of 2002 (HAVA) requires that each voting system "permit the voter to verify (in a private and independent manner) the votes selected by the voter on the ballot before the ballot is cast and counted." This is generally understood to mean that each DRE system should provide every voter with an opportunity to confirm his or her votes through an on-screen review of the voter's choices. This does relate to a voter verified paper audit trail (VVPAT), which would provide each voter a separate and additional opportunity to verify their selections by rereading those choices on a piece of paper.

HAVA also requires that each voting system "produce a permanent paper record with a manual audit capacity," and that the voting system "provide the voter with an opportunity to change the ballot or correct any error before the permanent paper record is produced."

This section is widely understood to mean that after voters confirm their votes via an on-screen review, and their ballots are cast, that a permanent paper record of each ballot be printed and kept by the local elections official in the case of a recount. HAVA is silent on whether this paper record should be printed concurrently with the on-screen confirmation, after the ballot is cast inside the machine, or at the end of the voting day once the polls close. And if printed concurrently with the voter's on-screen confirmation, HAVA does not speak to whether the paper record must be made available for each voter to verify their choices, or whether it should be printed inside the machine or at a separate printer without providing voter verification.

Currently there is one system certified in California that has a voter verified paper audit trail. This system allows a voter to review their choices using an on-screen display, and then to do a second confirmation on a printout which lists their voting choices. This printout can then be accepted by the voter, which casts the ballot, or rejected by the voter if the voter does not wish to cast those votes or if the voter believes there is a discrepancy between a vote they chose on the DRE screen and the vote shown on the printout.

The Task Force examined how the paper audit trail requirement should be accomplished, and whether the paper audit trail should be voter verified concurrent with the on-screen confirmation. A DRE system with a voter verified paper trail provides several security benefits in that it assures that the vote cast is accurate, and that any errors or inconsistencies between the DRE's electronic tally and the voter verified paper tally can be easily located and addressed.

However, voter verified paper audit trails impose greater administrative and technical needs, and so the Task Force also discussed voter verification options that do not involve paper. Very Important

LEGAL, TECHNICAL, AND PROCEDURAL CONSTRAINTS

As the Task Force discussed the issues of computer security, administrative security, voter confidence and voter verification, it became clear that several of these issues faced legal, technical and/or procedural constraints which posed, if not limitations, than at least some more questions.

1. FEDERAL AND STATE LAWS: ACCESSIBILITY FOR THE VISUALLY IMPAIRED, NO/LOW LITERACY VOTERS AND NON-ENGLISH SPEAKERS

Perhaps the most significant issue facing the development of any new voting system is the requirement in federal and state law that voting equipment provide blind and visually impaired voters with the ability to vote a secret ballot independently and without assistance.

The United States Congress, and the Legislature of the State of California, in enacting these requirements, clearly stated that this is a top priority and stipulated that federal and state funding shall be contingent on meeting this condition. In other words, the state, if it were to implement a ballot verification process that is not verifiable by blind voters, could place at risk the approximately $200 million the federal government is providing California for upgrading voting equipment and reform of the election process.

For all voting systems currently certified by the state, none has a paper-based voter verification option that can be utilized by blind, visually impaired, and illiterate or marginally literate voters, although several vendors have expressed the belief that such a process is feasible. Among the options vendors are exploring includes utilizing a fixed text reader that translates text to speech as the paper ballot is printed, or a reading pen

that would allow a blind voter to scan a pen across the paper print-out and hear the words spoken via a speech synthesis component in the pen.

Federal law also requires jurisdictions in California to produce election materials in languages other than English. The County of Los Angeles, for example, is required to provide ballots in English, Spanish, Chinese, Vietnamese, Tagalog, Japanese, and Korean. And Riverside County has a Cahuilla language requirement that is strictly an oral language and has no written form. Providing a paper-based representation of ballots in all these languages is also an important issue, as is the question of whether the paper-based representation must represent the ballot in English as well as the second language so that election officials can read the document.

The Task Force agrees that voting equipment should and must meet the requirements of federal and state laws requiring access to voting.

2. COURT ORDERED CONVERSION

A federal court order on the Secretary of State to assure that there are no pre-scored punch card systems in use in California beyond January 1, 2004, means that nine of California's counties must replace their punch card voting systems by that date. This can only be accomplished in conjunction with legal requirements for contracting and purchasing and the time limitations on state and federal certification of voting systems. For example, as of now, no voting systems currently certified by the state that provide for voting secretly and independently by persons who are blind include a voter verification option that the blind can utilize.

The Task Force agrees that the conversion process required by the presidential elections in 2004 must not be compromised and that its recommendations not undermine the successful preparation and administration of the upcoming March 2, 2004 primary election.

3. PRODUCT DEVELOPMENT AND TESTING CHALLENGES

In order for a county to purchase a system, the vendor would first have to develop it, submit it to national testing laboratories for security and other testing, and submit it to the state for similar testing and evaluation. In addition, the counties would have to issue Requests For Proposal, accept bids, analyze the bids, and negotiate a contract. Many counties are implementing a new voting system for local elections in November of 2003, only six months from the date of this report.

The Task Force agrees that the time requirements for product development and certification are significant issues in terms of the timing of the development of potential market solutions to address any of the issues brought up in this report.

4. DISASTER AVOIDANCE

Implementation of a new voting system requires – in order to avoid the missteps in the Florida 2002 election – significant time to train county personnel, train poll workers, educate the voters concerning the new voting systems, and otherwise prepare for the election. The likelihood that all of the steps outlined above could be accomplished in time to successfully install the equipment and successfully conduct an election in November 2003 is extremely remote.

The Task Force agrees that the presidential elections in 2004 must not be compromised, that any recommendations to change current voting equipment recognize the paramount importance of a successful election in terms of voter confidence, and that its recommendations not undermine the successful administration of those elections.

5. VOTER ISSUES

The California Constitution requires that voting be secret. Voting systems that rely on a "reel to reel" paper tape potentially order ballots sequentially, and could be amenable to efforts to determine which voter cast which ballot. In addition, in the absence of additional voting stations, there is the potential for increasing the time it takes to vote, creating longer lines at polling places, and discouraging voters from casting ballots.

There is unanimous concern on the Task Force that any proposed method of verification not inconvenience voters, create lines at the polling place, or otherwise discourage voters from casting a ballot.

6. ELECTION ADMINISTRATION

The recruitment and training of nearly 100,000 mostly elderly poll workers for a statewide election is a major undertaking under current circumstances. Requiring more complex equipment naturally raises concerns over poll worker recruitment, training, mechanical reliability, ongoing operational costs, and voter frustration. These concerns need to be considered.

The Task Force agrees that new equipment options should be as simple to administer as possible so as to not create unnecessary complexity at the polling place.

7. PRINTER ISSUES

One method discussed is to create a paper record of the vote for each voter to verify his or her ballot choices. This requires that a printer be added to the voting machine. The voting machine can produce the printed version of the ballot when the voter casts his or her ballot, when the polls close, or as required for the 1% manual recount. The latter two of these options are currently available on California-certified DRE systems.

Printers at polling places potentially create several significant election administration problems, including: (1) added cost to the system; (2) printer jams or other malfunctions requiring poll worker intervention; (3) added weight to the voting equipment; (4) current inaccessibility of the paper verification option to persons who are blind, visually impaired, illiterate, marginally literate, or are oral language restricted; (5) need for printers to print in foreign language characters; (6) more equipment that poll workers need to be trained to use and troubleshoot any problems; (7) more equipment for each jurisdiction to store, transport and maintain; and (8) additional supplies and warehousing procedures required to account for "official" ballot paper requirements. Battery/ Site Preparation @ Polling Place

The Task Force agrees that there are a number of logistical challenges that are present with any paper-based voting system using printers and these challenges need to be explored and understood in greater detail.

8. MARKETPLACE

As noted, there are currently no voting systems that offer paper-based voter verification procedures that provide persons who are blind or visually impaired with the ability to verify their ballot. Systems currently available, either as certified systems or as prototypes, rely on paper for a voter to verify the electronic record. The marketplace is potentially capable of addressing the technical issues with printers and poll workers listed above as well as producing solutions to achieving voter verification without utilizing paper.

The Task Force agrees that local jurisdictions should have a range of verification option to choose from, including paper-based and electronic options.

9. REIMBURSEMENT

As mentioned above, several counties have already purchased DRE voting equipment. New standards have been developed by the FEC and newer standards may be

developed by NIST. This presents potentially significant issues of funding and reimbursement, and raises the issue of the timing of any requirement for implementing new standards or acquiring new equipment.

The Task Force agrees that state or federal funds should be provided to pay the cost of upgrading any system that does not meet the requirements implemented as a result of the recommendations of this report.

RECOMMENDATIONS

The Task Force has agreed that there are four major areas deserving recommendations to the Secretary: Security, Paper Records, Voter Verification, and Independent Verification.

1. SECURITY

There are currently too many holes in the federal qualification and testing process that need to be strengthened in order for the Task Force to be confident that software is being developed, checked, tested, loaded, and run with adequate safeguards to prevent tampering or bugs.

After hearing from experts on computer security as well as election experts versed in election administration security procedures, and receiving no response from several inquiries to Wyle Laboratories and Ciber (two of the three federal ITAs that test DRE voting system hardware, software and firmware), the Task Force agrees that each of these areas is not as strong as they can and need to be.

In addition, some members of the Task Force have significant concerns about the security protocols that vendors have in place during the product development phase and throughout the vendor's participation in the modification and improvement of software and systems through software patches.

As such the Task Force makes the following recommendations to improve security and testing procedures at all levels:

A. Federal Testing

1. System security and integrity requirements must be more specifically defined at the Federal level. These requirements must assure a clean operating

environment both during the development process and during the operational phases while running an election, with no possibility of undetected intrusion at each point.

2. The ITA Qualification Tests must assure that the Federal requirements are met, to avoid duplication of testing effort by individual states.

3. A system designed to protect the most valuable aspect of our democracy – our voting systems, must be free from any questions over inadequacy, conflicts of interest, or collusion. Transparency is the only method that will ensure that the public does not question the intensity of the certification process. Therefore, the Federal testing process must increase transparency by incorporating citizen observation and participation and increasing public disclosure throughout the entire qualification process.

4. Testing of software and hardware is not a finite process. As technology evolves it becomes easier to hinder or intrude upon a system. Yet, software code in an election system that is tested at the Federal level, might be audited and tested once by an ITA, and if it passes and is never modified, may never be tested again. As such, the Federal testing and qualification process must allow for continuous improvement such as through periodic review and testing, instead of one-time testing.

5. Most current systems in California were certified using the Federal Elections Commission's 1990 standards, which were in place at the time of their certification. Earlier this year, new standards were adopted for the ITAs to use in testing election systems (known as the 2002 Standards). The Task Force agrees that all systems previously certified using the 1990 standards should be required to be retested by current standards. If a system certified under 1990 standards cannot meet the current standards, the Task Force would recommend that the state and federal governments provide funds to assist local jurisdictions in obtaining systems that are consistent with these standards. Such a replacement of the system should be done on a phased-in approach in order to avoid a problematic transition during an election.

6. Currently there is insufficient ongoing oversight of the ITAs to ensure that they are utilizing adequate quality control and maintaining the highest levels of scrutiny in testing election systems. The Task Force recommends that the National Institute of Standards and Technology (NIST), which the recently enacted Help America Vote Act of 2002 (HAVA) directs to establish federal standards, or the appropriate federal entity, conduct ongoing oversight of the ITAs.

7. Federal funding must be appropriated to enable NIST to conduct ITA oversight and to increase the technical security of systems.

8. Sometimes a large fraction of the software code, known as Commercial Off-The-Shelf (COTS) code because it is readily available for purchase to the public, is not audited at all. For systems without some form of voter verification, the blanket exemption for review of COTS code should be eliminated.

9. The Task Force recommends that NIST or the newly established Election Assistance Commission create a national database to track and document problems found in election systems, similar to Federal Aviation Administration incident reports, in order to keep local jurisdictions and the public informed.

B. State Testing

1. California certification tests are conducted or overseen by the Elections Division of the Secretary of State's Office. These certification tests must be focused on Elections Code and Election Division requirements. As such, the Election Division Regulations should assure that all ITA and NIST activities have been successfully completed as a prerequisite to certification testing.

2. The State should develop model Operational Security, Communications Security and Data Security procedures. Local jurisdictions should adapt the model procedures to their environments, and follow them in all elections operations.

3. When a vendor provides operating procedures for a system, they are often insufficient and incomplete. These operating procedures prepared by a vendor should include all operator functions required to assure proper operation in order to obtain certification.

4. Just as the Federal certification process must allow for continuous improvement such as thorough periodic review and testing, instead of one-time testing, so must the state certification process.

5. The Task Force acknowledges that its mission is limited by factors of time and knowledge. Therefore, the State should create a Technical Oversight Committee comprised of technical experts who can improve current testing and code-review standards, provide expert guidance throughout the certification process, and serve as a panel to review software and hardware issues that might arise. The panel members should be independent experts in computer science (especially computer security) and other engineering fields as appropriate who have technical expertise related to software development, computer security, user interface design, and other related fields. Panel members must not have financial or other conflicts of interest with voting equipment vendors. The panel should be convened by July 2003 and its meetings must be open to the public.

6. Like other states, California must require financial statements from applicants when they apply for certification.

7. The State must include a security analysis and a software analysis in its state certification.

8. The State must require the "threat analysis" from the federal ITA as part of all required documents before state testing of a vendor's system can begin.

9. To ensure that the code approved at the state and federal levels is identical to the code used at the local level, the State must require that the ITAs provide it with the executable code of each system to be tested. In addition,

the State must develop a system to compare that code with what a county uses on its machines for elections.

10. The State must obtain copies (either from the ITAs or from the vendors) of everything that each vendor provides to the ITAs, including source code, along with all the documents prepared by the ITAs during the Federal testing process. The Technical Oversight Panel (mentioned above in recommendation B(5)) should be able to review these documents at any time. All of these documents, except the source code and the threat analysis, would be public documents unless the vendor could establish that a document (or a potion thereof) meets certain standards of confidentiality or proprietariness established by the State, which would enable the document to be privileged. Those State standards should be made available to the public.

11. The State must conduct random audits of machines throughout the state to assure that software code in escrow with the State is the same code in use on each machine.

12. The State must conduct, or require local jurisdictions to conduct, random on-site sampling (otherwise known as "parallel monitoring") of a specific number of machines on Election Day to confirm that each system in operation is registering votes accurately. The procedures must be created by the Secretary of State in consultation with the Technical Oversight Committee mentioned in recommendation B(5). Protocols must also be in place in case a discrepancy is determined so that each jurisdiction using that type of machine can be notified promptly in order to take questionable systems out of service and the State can initiate an investigation.

13. The State must make voting system procedures, which are often adopted administratively, easier for the public to find and access. This could include adopting these in regulation or some other alternative such as publishing a readily available procedures manual or placing procedures on the Internet.

C. Local Testing

1. The integrity of the election process is based on the necessity, reliability, and comprehensiveness of the Federal and State certification procedures. As such, local jurisdictions that utilize systems that are not certified equipment or software must face State penalties.

2. State-approved communications security procedures are a pre-requisite to system-use in a live election. To ensure that hackers cannot intrude on a live system during voting, local jurisdictions must be on an isolated network. Furthermore, local jurisdictions should refrain from connecting voting machines to the Internet at any time.

3. The Logic and Accuracy process conducted at the local level must also be as reliable as the Federal and State tests. As such, the system vendor must not conduct these public tests.

D. Distribution of Software

1. The distribution of qualified voting system software should be tightly controlled. NIST should distribute qualified object and source code to the State, and the State, not the vendors, should control the distribution of object code to the local jurisdiction using that system.

2. Voting system vendors should not be permitted to alter object code without retesting and re-certification.

E. Technology

1. In order to minimize unintentional "undervotes," voters must be provided with a review screen on all DRE systems that provide them a reminder that they have not voted in or have skipped a particular race. This must also occur on any additional equipment providing audio for those with visual disabilities, illiterate voters, and those with limited manual dexterity.

F. Vendor Security

1. In order to assure that vendors are using programmers and designers of software that have only a commitment to creating the best product, and to prevent easily foreseeable problems for individuals with a clear history of criminal activity and/or mental instability, the State must require vendors to conduct background checks of programmers and developers before they are not hired to work on election system software. The State should establish the standards for these background checks, and the results of the checks must be made available to the State upon request.
2. The State must establish protocols and procedures for vendors to comply with, in order to guarantee that strict internal security procedures are used during their software development process. And vendors should be required to submit employee security procedures with their certification materials.
3. Vendors should be required to document a clear chain of custody for the handling of software to assure that all software and storage units containing software are handled, tested and transported in an appropriate manner.
4. The State must impose civil liability and stiff criminal penalties if any malicious code is found before, during, or after certification, whether such malicious code interferes with an election or simply was intended to. The liability and penalties must apply to the programmer or developer of the malicious code as well as to the vendor employing the individual(s).

2. Printing a Permanent Paper Record

Both Proposition 41 and the federal Help America Vote Act of 2002 (HAVA), seem to require a paper audit trail be prepared for each polling place.

Section 301(2)(B)(i) of HAVA states that a voting system must produce "a permanent paper record with a manual audit capacity." In addition, HAVA states "this paper record shall be available as an official record for any recount conducted with respect to any election in which the system is used."

Section 19234(e) of the Elections Code as passed by Proposition 41 states that "Any voting system purchased using bond funds that does not require a voter to directly mark on the ballot must produce, at the time the voter votes his or her ballot or at the time the polls are closed, a paper version or representation of the voted ballot or of all the ballots cast on a unit of the voting system. The paper version shall not be provided to the voter but shall be retained by elections officials for use during the one percent manual recount or other recount or contest."

While it may seem that this section of law requires a paper audit trail be printed, this provision has not been interpreted that way. The Secretary of State's Office and the Voting Modernization Board, created by Proposition 41, have interpreted this provision to mean only that a system have the 'capability' to print a paper record. In other words, if a DRE collects ballot images on a memory card, and a paper record can be printed later from the memory card, this has been deemed acceptable.

The Task Force agrees that to provide this required permanent paper record for each election, each local jurisdiction not using VVPAT should print out each voter's ballot as a record of the vote shortly after the closing of the polls. This process should be open to viewing by the public. For technical and logistical reasons there is no support to have the printing of this permanent paper record done at the time the ballot is cast (unless the system allows the voter to verify his or her vote on paper). These technical reasons include the potential for printer jams or printer failure, and limited time to adequately train volunteer poll workers how to fix printers in the middle of a hectic election.

Therefore the creation of the permanent paper record, if it is not a VVPAT, should be done once all ballots are cast. For research and statistical analysis purposes, each

local jurisdiction should provide these per-precinct ballot images to the State, which should make them available on CD-ROM at minimal cost to the public.

The Task Force also agrees that on all DRE systems, whether it includes a VVPAT option or not, that the electronic vote should be the legally valid vote unless there is some sort of discrepancy between it and the permanent paper record. The paper record would be used for the 1% manual recount mandated by California law. Then, if there is a recount or a challenge, there would be a 100% recount of the paper record. For the 1% manual recount and a full recount, the paper record should be presumed to be more reliable than the electronic vote unless there is evidence it has been corrupted or is incomplete. This would be true of any paper audit record produced, whether voter verified or not.

3. Voter Verified Paper Audit Trail

The issue of whether election systems should contain a voter verified paper audit trail (VVPAT) was one of the key questions discussed and debated by the Task Force. There was no consensus on the issue of whether a VVPAT should be required on all systems certified in California.

The Task Force includes individuals who are strong advocates for requiring a VVPAT not only to guard against software discrepancies or malicious code from creating problems in recording ballot choices, but also to identify other type of events which could upset the ballot count.

These advocates explain that stakeholders in our voting system -- voters, candidates and political parties -- must believe the voting system is secure and accurate if they are to have confidence in election outcomes. A fundamental component of voting system security is the ability to conduct a reliable audit of the election.

The advocates for VVPAT argue that there are three key criteria required to conduct a reliable election audit. Not only must there be a permanent record of each voter's ballot maintained for a period of time after the election (see Recommendation #2 above), but voters must be able to verify the accuracy of this permanent record and the audit process must be transparent.

The advocates for VVPAT believe that voters must be able to verify the accuracy of the permanent record because only the voter knows the true intent of their votes and how they cast their ballots. The only time voters can verify the accuracy of their ballots is while voting because once a ballot is cast, ballots become anonymous. The audit process must be transparent so that the permanent ballot records are visible to election stakeholders.

The Task Force members advocating for a VVPAT further explain that if election security is to be accepted by a wide variety of stakeholders and the public is to maintain its confidence in elections, then the audit process needs to be a reliable method that is widely understood. They explain that the most well-known and tested method for meeting these criteria is a paper-based audit system.

Currently, paper is the most widely used and understood medium for protecting valuable documents and verifying important transactions, such as those dealing with money, property and legal matters. The Task Force members supporting a VVPAT claim that if the permanent ballot record exists in an electronic, rather than paper format, that the electronic record could be easily altered after it has been verified and therefore is not a permanent record. No audit medium is tamper-proof, but they believe that a paper audit trail is more permanent and transparent than a digital audit trail that depends on software not readily apparent or understandable to stakeholders, particularly voters.

A voter's ballot is one of the most important documents that exists in a free society. The advocates for VVPAT say that to entrust this document to an entirely computerized system run on proprietary software (protected by trade secret) with no voter verified

paper audit trail is to ask voters, candidates (winners and losers alike) and parties to exercise blind trust in the voting system. Therefore, they feel that given the limitations of current technology, a voter-verified, paper audit trail is the only proven way to mitigate the real (and perceived) security risks inherent in any computerized voting system, such as programming errors, the use of unauthorized software, and deliberate attempts to manipulate an election.

Other Task Force members, though, are opposed to requiring a voter-verified paper audit trail because they argue that there are significant limitations on its implementation such as legal, technical and administrative constraints on how a VVPAT system would need to be designed.

Members of the Task Force opposing VVPAT suggest that printers add an increased technical burden at the polls since printers are often problematic, requiring on-the-spot troubleshooting during an election in the case of a problem. There are also added costs imposed on the State and counties to purchase, maintain and store printers, as well as to provide printing supplies.

In addition, those opposing a VVPAT requirement argue that there are legal burdens imposed on the design of each VVPAT system. For instance, HAVA requires that voting systems provide individuals with disabilities (especially the visually impaired) "the same opportunity for access and participation (including privacy and independence) as for other voters" and California Assembly Bill 2525 (Jackson), Chapter 950, Statutes of 2002, requires that blind voters be provided with "access that is equivalent to that provided to individuals who are not blind."

In addition, Section 2.2.7.2 of the Federal Election Commission's new 2002 standards specifies "DRE voting systems shall provide, as part of their configuration, the capability to provide access to voters with a broad range of disabilities. This capacity shall...provide audio information and stimulus that...provides instruction so that the

voter has the same vote capabilities and options as those provided by the system to individuals who are not using audio technology."

The opponents of requiring VVPAT argue that it is questionable whether providing a piece of paper to sighted voters to verify their choices while not providing a similar chance for verification for those with disabilities can be seen as "the same opportunity for access and participation (including privacy and independence) as for other voters," as "equivalent" access, or as "the same vote capabilities and options." Therefore, it remains an open question whether a VVPAT can be made to conform to these laws.

In addition, language access is also an issue since verification for non-English language voters would need to be in their preferred language. This can be difficult to accomplish while also ensuring that if a recount occurs the ballot can both be read by election officials and allow for secrecy (since there may be few voters casting ballots in that language). Printing bilingual ballots eases the readability issue, but does not address the secrecy issue. It also lengthens the size of the paper needed for verification.

Therefore the Task Force arrives at no consensus on the question of whether a voter verified paper audit trail (VVPAT) should be required. However, the Task Force agrees that systems with a VVPAT should be an option for local jurisdictions to choose, if such systems can meet the language accessibility requirements of HAVA, and the disability accessibility requirements of HAVA, AB 2525 and the FEC's 2002 standards.

For jurisdictions that choose to utilize systems with a VVPAT, there are several issues that must be addressed in order to give greater clarity to vendors, election officials and the public. The Task Force recommends that the state's Voting Systems and Procedures Panel, which is the state certification advisory body, address a series of issues related to VVPAT to ensure that all vendors utilizing such an option are conforming to consistent standards, and that conformity be a prerequisite of certification.

The issues to be addressed include, but may not be limited to, the following:

- ❑ Assuring randomized out-stacking of the paper ballot copies.
- ❑ Requiring adequate storage space and paper supply in each voting unit in order to accommodate the large number of ballots cast (and spoiled ballots) by the maximum number of voters allowed for each voting unit.
- ❑ Establishing design criteria for the paper ballot copies such as being easy for the voter to read, being in a format that lends itself to easy counting after the election, and determining the specific information to be included on the paper ballot copy.
- ❑ Establishing procedures that allow voters to reject or "spoil" their paper ballot copies.
- ❑ There will need to be procedures developed to enable voters who notice discrepancies to alert the precinct's poll workers. Such procedures would also need to stipulate under what conditions a voting machine would have to be taken offline.

4. Alternative Verification Methods

Because of reservations about paper-based voter verification, the Task Force wanted to encourage the development of alternative voter verification technology, such as fully electronic verification, that would ensure the security of each vote as well as provide greater voter confidence. Many (but not all) technologists feel that such alternatives could be developed and deployed within the next few years. The Task Force suggests that the State should explore urging, incentivizing, and possibly requiring vendors to develop such methods.

Until such time as alternative voter verification technology is readily available, voter confidence can be increased by following recommendation 1(b)(12) made earlier in this report regarding random on-site sampling of machines on Election Day (also known as Parallel Monitoring). Election Day sampling far exceeds the current testing methods in

use in California and elsewhere, and has a strong likelihood to detect potential machine tampering. The recommendation that each local jurisdiction make per-precinct ballot images available will also allow powerful post-election statistical analysis, which can provide evidence that even elections with surprising results reflect the will of the voters.

Because of the increased protections imposed by Election Day sampling, the Task Force agreed that there is time for vendors to develop voting systems with alternative voter verification of a ballot cast without paper. Electronic verification methods should preferably be within the machine to minimize extra equipment, and should not delay the time it takes to vote. The system should also be as voter friendly as possible and minimize any inconvenience or confusion to the voter. If feasible, it should provide the existing user interfaces while seamlessly including verification within the machine with little or no additional steps for voters to apply.

The Task Force agreed that there needs to be voter verification imposed by a date certain and the State and federal governments must provide funding to make this happen. There was disagreement, though over what type of voter verification audit mechanism to require, and on what timeline.

Six members of the Task Force would require an electronic verification method. These members believe that the technology is very close to developing an electronic voter verification audit mechanism for DREs that would not utilize paper. But these Task Force members want to provide enough time for the market to meet that need. They felt that it will take some time to perfect electronic verification audit methods, for these methods to be integrated into DREs, and for these methods to be federally qualified, state certified, and mass produced.

As such, this group of Task Force members recommends that the State allow vendors until December 31, 2006 to develop and obtain certification for such a solution, and at that point restrict vendors' ability to sell DRE systems without an electronic verification

feature. Therefore, all new systems purchased and put into use from January 2007 on must include an electronic verification audit feature that does not utilize paper.

But due to cost and the potential to create chaos in our electoral process, these members believe that the State should phase-in compliance for all jurisdictions that purchased DREs before 2007. And that all voting systems purchased prior to 2007 should be replaced with systems containing electronic verification or upgraded to include such a verification feature by 2010.

Three remaining Task Force members strongly agree with the idea of a voter-verified audit trail requirement (either with alternative verification or a voter verified paper audit trail), but feel a much greater sense of urgency about the timing of the conversion. This group feels that the state should impose such a requirement immediately, and that no additional DRE voting equipment should be purchased unless it meets that requirement. Counties that need to upgrade have several options available, including optical scan systems and DREs with printers (one such system is currently certified, and additional ones may be certified soon).

If a voter verified audit trail requirement is not imposed immediately, this group feels that it is vital that any new purchases of DREs be planned and budgeted with the conversion to this requirement in mind. To achieve this, this group believes that the State should mandate a voter-verified audit trail requirement (either with alternative verification or a voter verified paper audit trail), by January 2007 for all equipment deployed from now on (this deadline could be extended until 2010 for DREs currently in use). In addition, the state should strongly encourage all counties moving to deploy DRE voting systems to implement the requirement as soon as possible in advance of the deadline. Counties should negotiate those upgrades into their contracts, as Santa Clara County did in the contract signed at the end of April 2003, so that any additional costs due to the voter verified audit trail requirement can be covered by current Prop. 41 and HAVA funds.

This group is greatly concerned about the number of new purchases of DRE systems that are scheduled to occur before 2007. These Task Force members argue, that with these planned purchases, the number of California voters living in counties using DREs is expected to increase from about ten percent to over 50 percent by 2007. If a voter verification requirement does not take effect until 2010, this expansion will expose a majority of California voters' ballots to what these Task Force members believe to be serious security risks over the course of several major election cycles.

These Task Force members worry that if current plans come to pass, hundreds of millions of dollars of State and Federal funds will be expended on equipment that does not meet the proposed requirements. In 2010, the State will be faced with potentially large expenditures for upgrades. This cost may be so great that the voter verified audit requirements will be further delayed.

Therefore, the Task Force members are not far apart on imposing verification for all DRE systems in California – 3 years – and not far apart on the types of verification - with all members encouraged by the possibility of electronic or alternative verification methods, but three members believing that paper –based voter verification should be required immediately until electronic or other alternative voter verification methods are feasible.

All members also agree that prior to state certification testing, conformance with the electronic independent audit requirements should be determined by the Voting Systems and Procedures Panel, in consultation with the Technical Oversight Committee mentioned above. Before and after equipment has been acquired, the Voting Systems and Procedures Panel, in consultation with the Technical Oversight Committee, should have the power to ensure the integrity of verification audit mechanisms by ordering independent technical evaluations of voting equipment (including equipment that has already been fielded) at the expense of the vendor.

All information that the panel uses to arrive at its judgment on these audit mechanisms, including all design details of the audit mechanisms, including source code for any software they use, should be made public. The conclusions of the committee and the justifications for those conclusions must also be made public.

All the members also agreed that it is imperative that voter confidence in voting systems currently in use not be eroded by our efforts to add additional layers of security to the process. As such mechanisms are developed and certified, any adoption must be through careful integration into existing systems or part of system replacements and/or upgrades. Any state-mandated incorporation of independent electronic verification on existing systems must include full funding by the State or federal government for all costs.

CONCLUSIONS AND NEXT STEPS

The Task Force spent many hours exploring these issues and seeking to arrive at recommendations that were both responsible and feasible. Everything in this report is designed to increase the security of voting systems as well as to increase the confidence of the voters.

While there was not agreement on every issue the Task Force examined, we urge the Secretary, the members of the Voting Systems and Procedures Panel and others interested in the design, use, and security of voting systems to consider our recommendations, as all of them are the consensus of a committee that was incredibly diverse in our experience with voting systems, and our perspective on these issues.

We urge the Secretary to carefully review this report and to strongly urge the federal testing and standards authorities to consider our recommendations to improve the federal testing and qualification standards.

The Task Force also encourages the vendor community to review their security procedures – not only within the systems they are producing, but also the vendors' internal production and development security protocols, to make sure these are as strong as necessary given the importance that accurate election results are to our democracy.

Finally, we are quite cognizant that many of these recommendations will take substantial time and money to implement. We urge the federal and state governments to consider the considerable value that our society places on fair and accurate

elections, and to make an equivalent financial commitment over the necessary time period.

APPENDIX: Glossary of Terms

Acceptance Testing – the examination of voting systems and their components by the purchasing election authority in a simulated use environment to validate performance.

Accessibility – The ability of the voting system to be independently utilized by individuals with disabilities including those who are blind or visually disabled, without compromising the voter's privacy or secrecy of his or her ballot. The ability of the voting system to be independently utilized by individuals with alternative language needs pursuant to section 203 of the Voting Rights Act of 1965.

Accuracy – precision in recording, calculations and outputs.

Alternative Voter Verification – voter verification of a ballot cast using non-paper media (e.g. electronic voter verification).

Ballot Image – the detailed record of the selections made by a particular voter.

Certification Testing - the examination and testing of a voting system to determine its compliance with state laws and requirements for voting systems.

Commercial Off-The-Shelf (COTS) – software products as elements of larger systems that are readily available for sale by the public.

Data Security – the various methods and procedures, such as the use of passwords and encryption, implemented to prevent unauthorized use, destruction, or disclosure of data, whether accidental or deliberate.

Direct Recording Electronic (DRE) Equipment – an electronic voting device that captures votes/ballots at the point at which they are cast by the voter. This category includes all touch screen devices.

Early Voting – a form of absentee voting in which any voter may vote at the office of the elections official or at a satellite location as determined by the local elections official.

Election Assistance Commission (EAC) – established, as a result of the Help America Vote Act of 2002, to serve as a national clearinghouse and resource for the compilation of information and review of procedures with respect to the administration of federal elections.

Electronic Voter Verification – non-paper voter verification of a ballot cast, which utilizes trustworthy hardware (and possibly software) independent from the main vote capture program in order to provide independent confirmation of a voters' selections.

Escrow – the process by which a third party, having no direct or indirect financial interest with a vendor, holds the voting system software source code, including all changes or modifications and new or amended versions, for safekeeping and possible verification.

Federal Election Commission (FEC) – the body formerly responsible for producing the Federal Voting Systems Standards (FVSS). Its duties are now being separated and most of its voting functions will be assumed by the new Elections Assistance Commission (EAC).

Federal Voting Systems Standards (FVSS) – contains all the requirements for independent testing of voting systems.

HAVA – see Help America Vote Act of 2002.

Hardware – the mechanical, electrical and electronic assemblies, including materials and supplies, which are a part of the voting system. Hardware includes the voting device on which individual voters cast their ballot, as well as the actual equipment used to program ballot software or central vote tabulation software.

Help American Vote Act of 2002 (HAVA) – the federal election modernization law enacted in October 2002 which attempts to set national standards for elections and provides funding for the replacement of punch card and lever voting systems.

Independent Testing Authority (ITA) – testing laboratories, which can perform testing related to voting systems to meet the FVSS.

Logic and Accuracy (L&A) – the tests conducted to ascertain that the system will count properly the votes cast for all contests.

National Association of State Election Directors (NASED) – selects and approves testing laboratories which can perform testing related to voting systems to meet the FVSS.

National Institute of Standards and Technology (NIST) – the body, as directed under HAVA, that will conduct an evaluation of independent, non-federal laboratories to conduct testing, certification, de-certification, and re-certification of voting systems.

Object Code – the version of a computer program in the machine language of the computer on which it is to be used.

Operation Manual – a manual of all procedures used to prepare, operate and maintain the voting equipment, including the unpacking and storage procedures to be used by local elections officials.

Parallel Monitoring (also known as 'random on-site sampling' or 'Election Day

sampling') – a testing procedure in which voting machines are randomly taken out of service on Election Day and are voted on by State testers in order to simulate a true election and determine if the votes cast are correctly recorded. The testers would vote according to a prepared script in order to detect if the software is recording votes correctly.

Qualification Testing - testing at the national level by an ITA against the FEC's Federal Voting System Standards. Successful completion will place a vendor's product on a list of "Qualified" voting systems, meaning that they have been tested and found to meet or exceed the standards specified in the FVSS. Vote tabulation software, including source code, and election management software will be examined by a NASED approved ITA. The software ITA will handle any software that tabulates or reports votes and vote totals and which is not in a permanent machine resident status (on a ROM). This includes software that is resident on a computer hard drive or any software that is external to the voting system.

Software – the application and operating system programs associated with a computer or voting device, as opposed to hardware that refers to the physical components of a computer system. The term "software" includes any and all codes for operation of the vote counting system including ballot tabulation system bootstrap, monitor and device controllers, operating system, ballot layout, system audit, and report generation.

Source Code – the specific language a programmer uses to program the electronic equipment or vote tabulating system.

Test Deck – a pre-audited group of ballots voted with a pre-determined number of votes.

Vendor – any manufacturer, company, or individual who seeks to sell, or sells, a voting system or a vote tabulating system for use in California elections.

Voter Verified Paper Audit Trail (VVPAT) – a paper representation of a voter's choices that is verified by the voter at the time he or she casts his or her ballot.

Technical Oversight Committee – a committee proposed by the Ad Hoc Touch Screen Task Force that should be comprised of technical experts who can improve current testing standards, provide expert guidance throughout the certification process, and serve as a panel to review software and hardware issues that might arise.

Vote Tabulating Device – any piece of equipment, other than a voting machine, that compiles a total of votes cast by means of ballot card sorting, ballot card reading or scanning, paper ballot scanning, electronic data processing, or a combination of such equipment.

Vote Tabulating Program – the computer programs used for counting of votes cast on Ballots. It includes any and all vendor software, and the coding programs specific to each election.

Voting System – any mechanical, electro-mechanical, or electronic system and its software, or any combination of such, used to cast or to tabulate votes, or both.

Voting System Procedures – detailed procedures for operating a voting system adopted by the Voting Systems and Procedures Panel when a system is certified and available to the public.

SUBMITTAL

The undersigned members of the Ad Hoc Touch Screen Task Force hereby submit this Report to Secretary of State Kevin Shelley for his consideration:

/s/	/s/
Mark Kyle, Chair	Marc Carrel, Co-Chair
/s/	/s/
Kim Alexander	David Dill
/s/	/s/
David Jefferson	Robert Naegele
/s/	/s/
Shawn Casey O'Brien	Mischelle Townsend
/s/	/s/
Charlie Wallis	Jim Wisley

State of Maryland

State Board of Elections

Response to: Department of Legislative Services Trusted Agent Report on Diebold AccuVote-TS Voting System

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

January 29, 2004

A. Introduction

This document serves as the response of the Maryland State Board of Elections, the Administrator and her staff (SBE) to the Maryland Department of Legislative Services Trusted Agent Report on the Diebold AccuVote-TS Voting System. It contains four separate but interrelated sections:

A. Introduction,
B. Response to the "Red Team Exercise" Recommendations,
C. Response to "Further Recommendations", and
D. Notes (on statements made in the Report).

The Maryland State Board of Elections continues to be at the forefront of election reform, introducing a series of progressive reform measures, including authorization of provisional voting in the State, replacement of all remaining punch card and lever machines with Direct Recording Electronic (DRE) voting systems, continuous voter registration and partial implementation of a new Voter Registration System (VRS). As a result of these reform activities, the State is proudly regarded as a nationwide leader within the elections industry.

As a leader in new voting technology implementation, SBE accepts both its many benefits and occasional challenges. As the first state to open its DRE system to third-party, independent testing, we welcome the extensive external scrutiny provided by the Department of Legislative Services (through RABA Technologies) for the shared intent of providing voters of the State of Maryland undisputed confidence in the security of their vote.

Undeniably, no other state has taken such aggressive action as Maryland to address voting integrity concerns. Again, Maryland is leading the elections industry by taking unprecedented measures to ensure that the integrity of the intent of Maryland's voters is never compromised.

To this date, there has never been an election compromised. The findings in the SAIC and RABA reports both confirm the accuracy and security of Maryland's voting system and procedures as they exist today. In fact, Maryland's current voting system and procedures surpass current FEC guidelines. With that said, in our continued spirit of leadership, we embrace their recommendations for the assurance that the sanctity of future elections is preserved.

The SBE is confident that the Presidential Elections will be secure based on the following five factors:

1) **Demonstrated Success**: Over 20 successful elections have been conducted in Maryland using the DRE voting systems including the 2002 Gubernatorial Primary and General Elections.
2) **Existing Procedures**: Numerous management, operational, and technical controls are currently in place that protect the sanctity of the voting system.
3) **Enhanced Security:** Security recommendations in the SAIC Risk Assessment Report have been implemented by the SBE. In addition, SBE has addressed the default password issue that was suggested in the Trusted Agent Report.

4) **Management Action**: Additional security measures are being investigated to further ensure a successful Primary Election in March, such as the use of security guards, alarm systems, security cameras, lock boxes, tamper tape to seal entry points, and physical cages surrounding the servers to protect the county based GEMS servers and AccuVote-TS terminals from unauthorized use.
5) **Law:** Six sections in the Maryland Election Law Article address the illegality of tampering with the election process and/or the voting system. Persons caught tampering with election equipment as described in the RABA report, face punishment up to and including felony conviction under current Maryland statute.

B. Response to the "Red Team Exercise" Recommendations

The table contains the following information: **Category** and **RABA Recommendation** contain verbatim recommendations from the Trusted Agent Report; **SBE Mitigation Strategy** contains actions/strategies that SBE proposes to take in addition to Diebold corrective actions.

Category	RABA Recommendation	SBE Mitigation Strategy
Smart cards	1. Create Security Key Cards with computer-generated passwords *by precinct*. Update all the Encoders and AccuVote-TS terminals within each precinct.	▪ New security passwords and keys by county have been generated by SBE and will be implemented by the local boards of elections (LBEs) on all encoders and AccuVote-TS terminals during the Logic and Accuracy (L&A) testing process. ▪ With 1600+ precincts in the State of Maryland the recommendation, presented in the report, to implement security keys *by precinct* poses a greater risk to the efficiency and administration of the election process and could result in voters being disenfranchised from the election process. If incorrect security keys were provided to Election Judges, the voting units could not be set up for the election.
	2. Apply Tamper Tape to AccuVote-TS terminals to prevent non-authorized entry of Security Key Cards into the terminals.	▪ Attempts to tamper with terminals, via privacy security screen removal and unlocking of bay doors, would easily be recognized by the trained election judge and others in the polling place. The election judge's duty is to apprehend the individual for this felony criminal activity and contact police authorities. ▪ In addition to the above mentioned existing security measures, SBE is purchasing tamper tape and will instruct the LBEs to apply tamper tape to AccuVote-TS terminals during the Logic & Accuracy (L&A) tests and instruct the Election Judges to apply tamper tape after the units are activated on Election Day.

Category	RABA Recommendation	SBE Mitigation Strategy
	3. Institute strict procedures to prevent the use of unauthorized Supervisor Cards.	▪ Supervisor cards are sealed in separate envelopes that are only accessed by a pair of bi-partisan Chief Election Judges. ▪ To further enhance the security of the Supervisor's cards, SBE has developed physical security procedures and instructions for the LBEs and Election Judges.

301

Category	RABA Recommendation	SBE Mitigation Strategy
AccuVote-TS Terminals	1. Secure physical access to the voting terminal. The team recommends the use of serial-number tamper tape placed both inside and outside each locked bay. This could be accomplished in the following manner: after the terminals are loaded and a zero-tape printed the bay doors would be secured with the tamper tape and the serial numbers would be recorded. The tamper tape would need to be inspected periodically as a matter of procedure. Ultimately it would be recommended to place alarms on the bay doors.	▪ Further surpassing FEC guidelines and established best practices, SBE is purchasing the recommended tamper tape and will develop procedures for the LBEs to apply the tape, and procedures for periodic inspection of the AccuVote-TS terminal bay doors by the Election Judges.
	2. Remove the recording software from the AccuVote-TS terminal that allows the keyboard exploit. It serves no valid function.	▪ This software is mandated by the FEC Voting System Standards.
	3. Investigate the legal implications of tampering with the hardware systems (such as jamming the card reader and disconnecting the monitor). We see no short term fix for these attacks aside from the clear posting of rules that indicate consequences of such actions.	▪ Posters warning of the consequences of tampering with voting system hardware and software have already been purchased and the LBE's have already been instructed to place them in the polling places. Maryland Election Law Article, Subsections 16-206, 16-301, 16-801, 16-802, 16-803, and 16-804 apply to the illegal tampering of voting systems.

302

Category	RABA Recommendation	SBE Mitigation Strategy
GEMS Server	1. Install all known security patches from Microsoft on the GEMS servers.	▪ Additional security measures are being investigated to further ensure a successful Primary Election in March, such as the use of security guards, alarm systems, security cameras, lock boxes, tamper tape to seal entry points, and physical cages surrounding the servers to protect the county based GEMS servers and AccuVote-TS terminals from unauthorized use. ▪ ▪ SBE will assess what patches are necessary, based on the following considerations: • The GEMS servers are never connected to networks that have access to the Internet and are not vulnerable to attacks from unprotected networks. The recommended Microsoft security patches address systems that have access to unprotected networks. • The current version of GEMS software loaded on a Microsoft based operating system has undergone multiple tests by the Independent Testing Authorities and the State Board of Elections. • SBE's experience has demonstrated that making changes to the operating system can "break" GEMS. At this time, there is more risk with very little benefit associated with implementing patches without the opportunity to conduct thorough application testing with this GEMS system.

303

Category	RABA Recommendation	SBE Mitigation Strategy
	2. Ensure modem access to GEMS is enabled *only when uploads are expected,* i.e. via voice notification over a telephone line between a precinct judge and a designated LBE official. The number used for this purpose should be *guaranteed* not to change. Validate the number being dialed and the identities of the callers. The line should remain open until both sides indicate the upload is complete. Shut off the modems when not in use.	▪ SBE will instruct the LBEs that the procedures recommended by RABA are followed; however, upgrading the telephone systems to create enough capacity to accommodate this recommendation may be cost prohibitive for most counties. Additionally, implementation of this recommendation will likely cause a delay in the release of the unofficial results on election night. The following mitigation steps and procedures are already in place to address the concerns raised in this recommendation by RABA: ▪ The counties that use modems election night are required to establish procedures to re-read 100% of the PC memory cards and compare the unofficial results received by modem with the count produced by the PC memory cards. ▪ In accordance with established procedures, the tabulation of election results, a.k.a., "canvassing" is done four times: 1) Official polling place count, 2) First Absentee, 3) Provisional, and 4) Second Absentee, which includes votes from overseas personnel and provisional votes. These four tabulations combined become the *official* election results. ▪ At each tabulation, there are multiple checks and balances performed by the election judges and the local boards of elections in public forums to ensure that the votes are tallied correctly and that the number of votes cast equals the number of eligible voters who cast the ballots.

304

Category	RABA Recommendation	SBE Mitigation Strategy
		▪ Using Caller ID to verify election totals being transmitted from precinct to Local Boards of Election using modems: • Using caller ID technology can increase the security of receiving election totals via modem on election night. Verification of Election Judges who are responsible for election totals can be easily accomplished by using Caller ID and eliminate unauthorized transmission attempts by someone wanting to disrupt the election. • Verification of Election Judges and the approximate time each polling location transmits election totals will greatly increase the security of the use of modems. Caller ID technology is readily available using cellular phones and in many cases, existing phone systems in Local Boards of Elections.

305

Category	RABA Recommendation	SBE Mitigation Strategy
	3. Turn off all services and ports except those explicitly required by the GEMS software. For defense-in-depth install firewall software to block all ports except those required by the GEMS software.	▪ The GEMS servers are never connected to the Internet, therefore, no Internet "types of attacks" can occur since none of the voting system components are connected to an insecure network. ▪ SBE's experience has demonstrated that making changes to the operating system can "break" GEMS. At this time, there is more risk with very little benefit associated with implementing firewall software without the opportunity to conduct thorough application testing with this GEMS system.
	4. Update the anti-virus software.	▪ Completed. Anti-virus software on the GEMS servers in all 23 counties is current as of January 20, 2004.
	5. Turn off services that are not needed by GEMS.	▪ SBE's experience has demonstrated that making changes to the operating system can "break" GEMS. At this time, there is more risk with very little benefit associated with turning off services that are not needed by GEMS without the opportunity to conduct thorough application testing with this GEMS system.
	6. Install Tripwire on the system to provide an audit capability on the configuration.	▪ The GEMS servers have already been installed in the LBEs and the loading of the official ballots and Logic and Accuracy testing of the official ballots begins next week. To touch the GEMS servers now would be disruptive to the process and impact the completion of this process before the deadline for delivering the touch screen terminals to the polling places.
	7. Disable the "autorun" feature in Windows 2000 (change the value from 1 to 0 for the registry key: HKEY-LOCAL_ MACHINE\System\CurrentControlSet\Services\ CDRom).	▪ SBE has purchased tamper tape and will instruct the LBEs to put the tamper tape on the CD drive doors of the servers so that unauthorized software cannot be installed without detection ▪ SBE will implement the recommendation.
	8. Ensure the front panel on the server is locked and the server is stored in a physically secure location. Apply tamper tape to the input devices and the reboot button.	▪ SBE has purchased tamper tape and will instruct the LBEs to apply the tamper tape to the input devices and the reboot buttons of the servers. ▪ All GEMS servers are stored in physically locked locations.

306

Category	RABA Recommendation	SBE Mitigation Strategy
	9. Change the boot order to make the hard drive first AND password protect the BIOS to prevent changes to the boot order without physically opening the server.	▪ SBE has purchased tamper tape and will instruct the LBEs to apply the tamper tape to the front panel of each GEMS server. This will prevent access to CD and floppy drives. SBE will instruct those LBEs with GEMS servers that do not have a front panel to apply tamper tape over the CD and floppy drives. ▪ SBE will ensure the BIOS configuration is changed on each GEMS server to prevent installing unauthorized software. SBE will ensure each GEMS server has password protection applied to the BIOS configuration utility.

C. Response to "Further Recommendations"

The State Board of Elections, the Administrator and her staff will continue to work with Diebold and SBE's Security Consultant to assess the appropriate action to take in addressing the Red Team's "Further Recommendations".

D. NOTES:

- *State of Maryland Diebold AccuVote-TS Voting System Security Action Plan* was updated on January 20, 2004 to reflect that all tasks but one have been completed. The unfinished Task 10, which requires that a risk assessment be completed when software changes have been made, is waiting for signatures on a Non-Disclosure Agreement between DBM and BSC Systems, Inc. BSC Systems, Inc. is assisting SBE in developing its Information Systems Security Plan and cannot perform the risk assessment until it receives the un-redacted version of the *Risk Assessment Report, Diebold AccuVote-TS System and Processes* (developed by SAIC).
- SBE is verifying that existing procedures meet or exceed the FEC Voting System Standards Volume I requirements.
- At the time of SBE's interview with RABA Technologies, documentation of the actions SBE has taken to address the thirty-five requirements that SAIC labeled either unmet or partially met had not been formalized by SBE. Since that time, SBE has compiled the requirements into an "easily review able form" that is not "scattered".
- Valid Voter Access Cards cannot be "forged" unless a person knows the security keys and password. SBE has implemented the security feature of the Diebold AccuVote-TS voting system that changes the "fixed" password to a unique key for each county and is known only to two SBE personnel.
- The PCMCIA card is encrypted by keys chosen by SBE and is known only to two SBE personnel. The default key that has been published on the Internet is NOT used in Maryland.
- Election officials received basic security awareness training in October 2003. Training of the LBE election officials is on going. Security is incorporated in the Election Judges Training Manual and in the actual training classes. Election judges will be provided with a Security Checklist, including the procedures implemented as a result of this report, at the time they pick up their polling place materials prior to Election Day.