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

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

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. xx.

[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.