Order Code RL33190

CRS Report for Congress
Received through the CRS Web

The Direct Recording Electronic Voting Machine (DRE) Controversy: FAQs and Misperceptions

December 14, 2005

Eric A. Fischer
Senior Specialist in Science and Technology
Resources, Science, and Industry Division

Kevin J. Coleman
Analyst in American National Government
Government and Finance Division

The Direct Recording Electronic Voting Machine (DRE) Controversy: FAQs and Misperceptions

Summary

Most voting systems used in U.S. elections rely on computers in some way. The most computerized is the direct recording electronic voting machine, or DRE. In this system, votes are recorded directly onto computer memory devices. While DREs have been in use since the early 1990s, questions about their security and reliability were previously a relatively minor issue, even following the November 2000 presidential election and the subsequent congressional deliberations leading to the enactment of the Help America Vote Act of 2002 (HAVA, P.L. 107-252).

However, at least two factors led to a sharp increase in public concerns about DREs beginning in 2003. First, the voting accessibility provisions in HAVA promote the use of DREs, which have been the only kind of voting system that can meet the HAVA requirements to permit persons with disabilities, including blindness, to vote privately and independently. Second, potential security vulnerabilities with DREs were publicized as a result of several studies. Several bills have been introduced in the 109th Congress that would address these issues in different ways.

In the public debate about DREs, there has been some confusion about what the problems and issues are, arising to a significant degree from the complexity of DREs and of elections in general. This confusion can lead to misperceptions about facts as well as issues and options for resolving them. Points worth noting include the following:

DREs do have unique security concerns and have not been thoroughly tested in the scientific community. However, most election problems in 2004 were not associated with DREs. Security flaws in them are not known to have compromised any elections, and it is not clear how much of a threat those vulnerabilities pose to election integrity in practice, especially in comparison to other kinds of threats. The different models of DREs in current use vary substantially in design, and problems that one model exhibits may not occur in others. Many of those problems are procedural, not weaknesses in the technology itself.

It is not clear whether the unique security problems posed by DREs are best addressed by requiring that they produce paper ballots or by other means. While paper has useful security properties and is well-known, other methods exist that might be superior. Furthermore, paper ballots used with DREs (called voter-verified paper audit trails, or VVPAT) are largely unproven and it is not clear how well they can meet HAVA requirements for accessibility or other goals such as usability.

As Congress considers proposals relating to DREs, salient issues might include the lack of information about DRE security, especially in relation to other systems and other components of election integrity; potential conflicts with HAVA requirements that might be associated with the proposals; how those proposals might impact voter confidence; and what impacts they might have on future innovation. This report will be updated in response to major developments.

Contents

The Direct Recording Electronic Voting Machine (DRE) Controversy: FAQs and Misperceptions

Most voting systems used in federal, state, and local elections in the United States rely on computers in some way. The most computerized is the direct recording electronic voting machine, in which votes are recorded directly onto computer memory devices. DREs are the most technologically advanced of current voting systems. They and other forms of electronic voting offer substantial promise for improving elections for both voters and election officials.[1]

Questions about the security and reliability of DREs were a relatively minor issue until the past two years. Two factors led to a sharp increase in public concerns about them: (1) the Help America Vote Act of 2002 (HAVA) prequires at least one voting machine in each precinct to fully accommodate disabled voters and DREs are the only system that currently meets this requirement; and (2) the security vulnerabilities of DREs were widely publicized as the result of several studies released in 2003.[2]

Much of the debate over DREs has focused on whether they should be required to produce a paper ballot that can be verified by the voter as a solution to potential vulnerabilities. This approach is often called the voter-verified paper audit trail (VVPAT). Bills to require VVPAT were introduced in the 108th and 109th Congresses, but there is divided opinion about both VVPAT and the security vulnerabilities of DREs, particularly with respect to the comparative vulnerabilities of other voting methods and various other aspects of election administration. Proposals to require that DREs use VVPAT have been seen by some observers as the method of choice for addressing the concerns. However, others, including many election officials[3] believe that VVPAT is unnecessary or even counterproductive and that security issues are best addressed through other approaches.

The public debate about DREs and VVPAT has led to some confusion about the problems and issues involved, and as a consequence, the options that might resolve

---

[1] See, for example, Caltech/MIT Voting Technology Project, *Voting: What is, what could be,* July 2001, [http://www.vote.caltech.edu/reports/2001report]; National Research Council, *Asking the Right Questions about Electronic Voting,* (Washington, DC: National Academies Press, 2005).

[2] For in-depth discussion, see CRS Report RL32139, *Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues,* by Eric A. Fischer.

[3] See, for example, CRS Report RL32938, *What Do Local Election Officials Think about Election Reform?: Results of a Survey,* by Eric A. Fischer and Kevin J. Coleman.

them. The questions and answers that follow address selected issues and misperceptions concerning DREs and VVPAT, in an effort to clarify and inform the ongoing policy discussion.

FAQs and Misperceptions

Questions that arise frequently with respect to the controversy surrounding DREs and possible misperceptions in the debate can be classified into three categories: those relating to DREs themselves, those that relate to paper audit trails, and those that relate to recounts and audits. Questions in each of those categories are addressed in turn below.

Problems with DREs

Were DREs the source of most election problems in 2004? Voters in various jurisdictions across the country experienced difficulties with the voting process in the November 2004 election, but problems with DREs were a comparatively minor issue on the whole. Both during and after the election, the media reported issues with voter registration, the rules for counting provisional ballots, the length of time required to vote, absentee ballot problems, and allegations of voter intimidation and fraud, along with reports about DRE malfunctions of voting equipment, including DREs.

A number of malfunctions relating to DREs were covered prominently in media reports on election problems, particularly problems in Franklin County, Ohio, and Carteret County, North Carolina (discussed in greater detail below). However, only the latter involved a problem with DREs per se. Various glitches and procedural problems were reported with DREs in other states as well, but machine malfunctions that could not be attributed to human error were the exception according to a compilation of media reports by the Election Reform Information Project.[4]

In comparison, many problems were associated with provisional and absentee ballots. A survey[5] sponsored by the federal Election Assistance Commission (EAC) and performed by Election Data Services[6] found that at least 1.9 million voters cast provisional ballots nationwide, which were counted or not according to different rules in the various states. In Ohio, which required that a provisional ballot be cast in the voter's home precinct, approximately 22% of the 157,714 provisional ballots cast in the state were not counted (nearly 34,000 ballots). The percentage of provisional ballots counted by states ranged from 0% (Idaho) to 100% (Maine), with an average of about 50%.

---

[4] Election Reform Information Project, *The 2004 Election*, December 2004, [http://www.electionline.org/Portals/1/Publications/Election%20Reform%20Briefing%209.pdf].

[5] Election Assistance Commission, "Election Day Survey," October 3, 2005, [http://www.eac.gov/election_survey_2004/toc.htm].

[6] EDS [http://www.electiondataservices.com] is a private consulting firm founded in 1977 that works on election administration, redistricting, and related matters.

With respect to military and overseas voters, a survey of 761 local election officials by the National Defense Committee, a private organization, reported that 126,952 absentee ballots were mailed to members of the military and citizens living abroad, of which 94,359 were returned and counted.[7] More than 30,000 of the absentee ballots in this survey (approximately 26%) were not returned at all, were disqualified for procedural reasons, or were returned too late to be counted.

Long lines also plagued voters in many states, with some waiting hours to cast a ballot (one Ohio voter reportedly waited 10 hours to vote). While it is impossible to know how many voters abandoned lines without voting, long lines impede the voting process and create a final obstacle at the polling place for those who turn out to vote.[8]

Among other sources, the Election Incident Reporting System, affiliated with the Verified Voting Foundation, a VVPAT advocate, recorded 42,841 complaints about the election, 11% of them relating in whole or part to voting machines.[9] Most of the complaints in that data set relate to registration or polling place problems.

Have DREs been thoroughly tested in the scientific community? DREs have been tested by scientists, but the systems have not generally undergone the kind of open scientific scrutiny that might be expected. They are proprietary machines, and manufacturers require confidentiality agreements of those who wish to acquire them. Testing is done as part of federal and state certification processes, but detailed results are not publicly available. More detail has been provided in only a relatively few cases — especially, the analysis of software obtained from a manufacturer's unsecured website in 2003, and subsequent studies by the states of Maryland and Ohio.[10] Additional studies are ongoing.

---

[7] National Defense Committee, *Military and Overseas Absentee Voting in the 2004 Presidential Election*, Mar. 30, 2005, [http://www.nationaldefensecommittee.org/pages/absentee_voting.html].

[8] Many states require that employers provide employees time off to vote, generally about two hours during the time the polls are open. Additional time to vote, if an employer permitted it, would likely be unpaid time. Long lines may also make voting more difficult for certain disabled voters.

[9] Election Incident Reporting System, "Nationwide Election Incidents: Election Year 2004," [https://voteprotect.org/index.php?display=EIRMapNation&cat=ALL&search=&go=Apply+filter&tab=ED04], n.d.

[10] 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.pdf]; 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_publishing/public_content/dbm_search/technology/toc_voting_system_report/votingsystemreportfinal.pdf]; Maryland Department of Legislative Services, "A Review of Issues Relating to the Diebold AccuVote-TS Voting System in Maryland," January 2004, [http://mlis.state.md.us/Other/voting_system/final_diebold.pdf]; Maryland Department of

(continued...)

HAVA has established some procedures, including the formal involvement of the National Institute of Standards and Technology (NIST) and the science and technology communities, in the standards-development and certification processes (§214 and §221). These and other factors may lead to an increase in the involvement of scientists in the study of DREs and other aspects of election administration. That has already happened to some extent, with, for example, the establishment of the Voting Technology Project by the California Institute of Technology and the Massachusetts Institute of Technology,[11] the involvement of the American Association for the Advancement of Science (AAAS) in election reform issues,[12] and the awarding of a major grant by the National Science Foundation to several institutions to establish a center for voting technology research.[13]

Are there any unique security concerns with DREs? DREs currently in use have a unique security vulnerability. It results from the same feature — reliance on a computer for casting and recording of votes in a single machine — that gives DREs their capabilities in accessibility, usability, and efficiency. Because the machines rely on complicated software, it is at least theoretically possible that someone could insert hidden computer code that would add, subtract, or change votes. There are several things that such malicious code, or malware, might do. In the best known potential exploit, the hidden code would cause the DRE to record a different vote from what the voter sees on the face of the machine. Another possibility is that the malware could change vote totals after they had been recorded but before they are downloaded for tallying.

While an optical scan or punchcard counter could also be programmed to record a different vote from that intended by the voter, with those systems the ballot that the voter saw is preserved as part of normal practice and can be checked independently by another machine or a human. That is not possible with a DRE, where the choices the voter sees on the face of the machine are ephemeral — they are reset when the voter casts the ballot. The actual record of the voter, preserved on an electronic medium, is not something the voter ever sees. In that way, DREs are like lever machine voting systems, in which casting a ballot advances mechanical counters, which the voter cannot see, and resets the levers for the next voter. The difference is that any tampering with lever machines would have to be done one machine at a

---

[10] (...continued)
Legislative Services, "Trusted Agent Report: Diebold AccuVote-TS Voting System," prepared by RABA Technologies Innovative Solution Cell, 20 January 2004, [http://mlis.state.md.us/Other/voting_system/trusted_agent_report.pdf]; Ohio Secretary of State, "Statewide Voting Systems," October 18, 2005, [http://www.sos.state.oh.us/sos/HAVA/hava.aspx?section=4].

[11] Caltech-MIT/Voting Technology Project, [http://www.vote.caltech.edu].

[12] See, for example, Committee on Scientific Freedom and Responsibility, American Association for the Advancement of Science, "Statement on the Importance of Research on the U.S. Voting System," February 2005, available at [http://www.aaas.org/spp/sfrl/committees/csfr/VotingStatement.pdf].

[13] The institutions involved include five universities — Johns Hopkins, Rice, Stanford, California at Berkeley, and Iowa — and SRI International See Avi Rubin, "ACCURATE," [http://accurate-voting.org], September 30, 2005.

time, whereas malicious code need be inserted into DRE software only once, before it is loaded onto the machines. As with lever machines, lost or changed votes could result from malfunction as well as intentional tampering.

It is generally recognized that this vulnerability of DREs poses at least a theoretical risk. The controversy arises over whether it poses a significant risk in practice, and, if so, what is the most appropriate response. Some DRE proponents claim, for example, that the design of DREs prevents the writing of malware that could change votes in a predictable way. Others claim that following appropriate security and audit procedures is sufficient to prevent successful tampering and that modern DREs, when properly managed, have less risk of losing votes through malfunction than any other voting system. Most DRE critics state, in contrast, that those claims are wrong or cannot be substantiated, and that the only effective solution is a permanent paper ballot that the voter has verified. Other critics state that there are effective alternatives to paper ballots that may be superior to them. In fact, most experts believe that it is impossible to prove that a complex system, such as a DRE or any other voting system,[14] is secure against all possible threats. The question is rather whether they can be made sufficiently secure to make the risk from attempts at tampering acceptably low.

Have DRE security flaws compromised any elections? There were no substantiated reports from any state of compromised elections due to security flaws that involved computer hacking or similar attacks in 2004.[15] As one observer has noted, "Unlike paper ballots, in the history of DREs, no one has found any evidence of the machines being used for fraudulent purposes."[16] Malfunctions occur, but most problems with DREs can be attributed to human mistakes or procedural errors, rather than security issues. In one of the most celebrated DRE malfunctions in 2004, voting machines in Carteret County, North Carolina, stopped counting ballots once 3,005 voters had voted, although they appeared to continue accepting votes. Poll workers expected the machines to accommodate 10,000 voters. An estimated 4,500 votes were lost as a result, attributable to a lack of human oversight in upgrading machine capacities rather than a security breach or an attempt to commit

---

[14] Even the most technologically unsophisticated voting system — the hand-counted paper ballot — is complex in practice because of the procedures required to generate, control, cast, and count the ballots.

[15] Just after the November 2004 election, a New York Times article about electronic voting problems noted that "There is also no way to be sure that the nightmare scenario of electronic voting critics did not occur: votes surreptitiously shifted from one candidate to another inside the machines, by secret software…It's important to make clear that there is no evidence such a thing happened, but there will be concern and conspiracy theories until all software used in elections is made public." ("About Those Election Results," *New York Times*, November 14, 2004). Whether making voting-system software available for public inspection is the best or even an appropriate solution to security concerns remains controversial (CRS Report RL32139, *Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues*, by Eric A. Fischer).

[16] Arrison, Sonia, "In Praise of E-Voting Machines," July 8, 2005, [http://www.technewsworld.com/story/44476.html].

fraud.[17] Because of a close vote in one county race, a second election was required to resolve the contest, a very rare occurrence.

The widely reported problem of an overcount in Franklin County, OH, occurred when a laptop was used in a precinct to communicate the unofficial tallies from a DRE memory cartridge to the central office. The total number of voters casting ballots in the precinct was 638, but the number initially reported as casting a vote for President exceeded 4,500. The memory cartridge itself and other redundant memory for the DRE contained the correct count, and the error was quickly discovered and corrected.[18] The problem was diagnosed by the DRE vendor as a technical flaw relating to communication between the memory cartridge and the laptop, and controls were added to prevent the problem in future.[19]

Aside from the unique security challenges posed by DREs, human interaction with electronic voting machines involves a chain of custody that parallels any other type of voting equipment or method. In this regard, there have been reports of questionable behavior by poll workers, election officials, and vendors with respect to DREs, as with other voting methods. It is not likely that most poll workers possess the knowledge to alter lever, optical scan, or electronic voting machines, and security measures should be designed to address the unique characteristics of each type of voting system to prevent tampering and fraud. Nevertheless, some observers point out that a successful attempt to tamper with DRE software may be especially difficult to detect. If so, discovery of any resultant fraud would be unlikely. Some also believe that the threshold for investigation of possible election fraud is too high in many states and that, as a result, many attempts at tampering may go undetected, no matter what voting system is used.

Do security flaws in DREs pose the greatest threat to election integrity? While current DREs have unique security flaws, it has not been established that they pose a greater threat to the integrity of elections than other kinds of problems. The unique concern about DREs and, to a lesser extent, other computer-assisted voting systems, such as optical scan, is the risk from malware, described above. Some experts and activists are concerned that hidden malware could be successfully implanted by an insider, during manufacture or at some other point before distribution, and could be used to impact elections at the national level. For this reason, some observers consider security flaws in DREs to be of major concern to the integrity of elections.

---

[17] Mark Schreiner, "N.C. Electronic Voting Tallies Up Widespread Confusion," *Wilmington Star-News*, Nov. 17, 2004.

[18] Robert Vitale, "No New Discrepancies Found in Vote Tally," *The Columbus Dispatch*, November 27, 2004.

[19] Board of Elections, Franklin County, Ohio, "ELECTION 2004: A Report to the Community," February 11, 2005, available at [http://www.electionline.org/Portals/1/Resource%20Library/Franklin.County.OH.2004.pdf].

All voting systems have security vulnerabilities, and DREs are currently used by only about one-fourth of voters nationwide.[20] In contrast, optical scan systems are used by about 40% of voters, and security vulnerabilities have also been demonstrated with optical scan counters.[21] However, the proportion of voters using DREs is expected to increase as a result of HAVA's accessibility requirements, since DREs are currently the only kind of voting system that is generally agreed to meet those requirements.

There are many other potential threats to the integrity of elections. Most are not related to voting-system technology.[22] Possible threats include such things as voter-registration fraud, voter intimidation and misdirection, absentee-ballot fraud, flawed election procedures, poor ballot design, poor functional design or maintenance of voting equipment, and significant procedural error. Recent evidence indicates that most lost votes result from voter registration, polling place, and usability problems, not security issues.[23] Some experts argue that such flaws pose a greater threat to the integrity of elections than recent concerns about DRE security, and too much attention is currently being paid to the latter. Unfortunately, there does not appear to be sufficient information available to determine objectively which kinds of threat should be of highest priority to counter.

Do all types of DREs have the same problems? DREs are actually more diverse than any other kind of voting system currently in use. There are several different kinds, by several different manufacturers. First introduced in the 1970s, the systems vary significantly in age, capability, and features. Some present voters with a full-face ballot and register choices via microswitches that the voter presses. Others present ballot pages on a computer screen and register choices via a touchscreen mechanism, point-and-click device, or some other mechanical method. Only more recently manufactured DREs have accessibility features for persons with disabilities. Older models are also more likely to have problems and may have been the source of most of the lost votes attributed to this kind of voting system in the 2000 election.[24]

---

[20] Election Assistance Commission, "Election Day Survey," October 3, 2005, [http://www.eac.gov/election_survey_2004/toc.htm].

[21] See, for example, Harri Hursti, "Critical Security Issues with Diebold Optical Scan Design," *The Black Box Report*, July 4, 2005, [http://www.blackboxvoting.org/BBVreport.pdf].

[22] For a discussion of technological and some other threats, see National Institute of Standards and Technology, "Developing an Analysis of Threats to Voting Systems," October 7, 2005, [http://vote.nist.gov/threats/index.html].

[23] Caltech/MIT Voting Technology Project, *Voting: What Is, What Could Be*, July 2001, [http://www.vote.caltech.edu/reports/2001report]; Charles Stewart III, "Residual Vote in the 2004 Election," Caltech/MIT Voting Technology Project Working Paper #25, February 2005, [http://vote.caltech.edu/media/documents/wps/vtp_wp25.pdf].

[24] The Caltech/MIT Voting Technology Project, "Residual Votes Attributable to Technology: An Assessment of the Reliability of Existing Voting Equipment," VTP Working Paper #2, March 2001,

(continued...)

While at some level DREs all share the vulnerability to malware discussed above, security features and vulnerabilities also vary among types and models of DRE. Consequently, a failure or weakness identified or experienced with one particular system will not necessarily be applicable to others.[25] That is also true with respect to other technological issues such as reliability. For example, the DREs that failed in Carteret County, NC (discussed above), were an older model with more limited computer memory than more recent systems.

Do problems with DREs result from weaknesses in the technology itself? DREs have vulnerabilities, as noted above, but most of the incidents identified with those voting machines appear to have resulted from procedural problems rather than any inherent weakness in DRE technology itself.[26] DREs are computer-based systems, as are optical scan counters, many voter registration databases (as required in all states by HAVA starting in January 2006), and other aspects of election administration, and they are subject to the same problems as any computer-based system. But preventable problems that result from human error, such as administrative or procedural mistakes, and problems that occur with optical scan ballot counters, not DREs, are often conflated in the public eye with weaknesses in DRE technology.[27]

Available evidence also indicates that DREs, when properly implemented, can provide performance substantially superior to the systems they replace. A study on the residual vote rate (the percentage of ballots that did not record a vote for President) between 2000 and 2004 found that jurisdictions that changed to DREs from any type of voting system lowered the rate, particularly those changing from punch cards to DREs.[28] While any change in voting system reduced the residual vote rate, DREs performed comparatively well by this measure. Although the residual

---

[24] (...continued)
[http://vote.caltech.edu/media/documents/wps/vtp_wp2.pdf].

[25] For example, if the data used to draw the ballot on the computer screen are stored in graphic rather than text format, it may be more difficult for malware planted upstream from the election jurisdiction to identify the candidates or their affiliations.

[26] Also, most of the cited security and reliability weaknesses for DREs and optical scan systems summarized in a recent Government Accountability Office study were procedural and administrative — and included vendors, testing authorities, and election administrators — although significant technology flaws were also reported (Government Accountability Office, *Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed*, GAO-05-956, September 2005, [http://www.gao.gov/new.items/d05956.pdf]).

[27] For example, one of the most critical recent accounts of electronic voting includes a list of more than 100 examples of problems, culled from media reports and other sources. The list combines various kinds of problems with DREs and optical scan counters and does not provide an analysis of the kind of system with which the problem occurred or the cause (Bev Harris, *Black Box Voting: Ballot Tampering in the 21st Century* (High Point, North Carolina: Plan Nine Publishing, 2003), p. 16 — 55).

[28] The largest drop in the residual vote rate was 1.46% (punch cards to DREs), and the smallest was 0.61% (no change in voting equipment). Charles Stewart III, *Residual Vote in the 2004 Election*, Caltech/MIT Voting Technology Project, February 2005.

vote rate is an imperfect measure because some voters skip the presidential race, it does provide some evidence of voting system performance.

Is certification of DREs under federal and state voting system standards sufficient to make them secure? In general, certification standards with appropriate security provisions are considered to be necessary but not sufficient to achieve an acceptable level of security. They provide only a baseline of features, controls, and performance that a system should exhibit as part of an overall security strategy. The DREs in which security vulnerabilities had been discovered in the studies cited above had in fact been certified under the federal voting system standards (VSS).[29] While it is not clear whether the certification testing of those systems identified any of the problems that were discovered in the recent studies, the process did not in any case prevent those systems from being certified and deployed with the vulnerabilities present.

The Election Assistance Commission guidelines (called the Voluntary Voting System Guidelines or VVSG) that will replace the VSS have more extensive security requirements,[30] but the above example shows that certification alone is not sufficient protection against security vulnerabilities, and it is not generally considered to be so. There are at least two reasons for this. First, the security threat environment for information technology in general is constantly evolving, with new threats arising on a regular basis. Consequently, it is unrealistic to expect certification under a comparatively static standard to anticipate and protect against all new kinds of threats that may arise against voting systems that rely on information technology. Second, the VVSG process leads to certification of technology, but procedures and personnel are equally important to effective security and often pose significant vulnerabilities.[31] In addition, standards often require compromise to balance different functions and goals — such as accuracy, security, speed, usability, and cost — and unless security is considered paramount, it will of necessity be subject to such compromise.

Voter-Verified Paper Audit Trails (VVPAT)

Can DREs be made sufficiently secure without a paper ballot? If the vulnerabilities discussed above pose a significant risk for DREs in practice, there are methods other than adding paper ballots which could be used to address them. Unfortunately, none of these methods, including paper, have been sufficiently developed to compare efficacy, practicality, and cost in a meaningful way.

---

[29] These voluntary standards were developed under the auspices of the Federal Election Commission., with the most recent version released in 2002 (see CRS Report RS21156, *Federal Voting Systems Standards and Guidelines: Congressional Deliberations, by* Eric A. Fischer). However, the tested systems had been certified under the 1990 VSS, which had a much less extensive section on security.

[30] See CRS Report RL33146, *Federal Voluntary Voting System Guidelines: Summary and Analysis of Issues,* by Eric A. Fischer.

[31] See CRS Report RL32777, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options,* by Eric A. Fischer.

Paper ballots used with DREs — usually called a voter-verified paper audit trail, or VVPAT — provide a permanent, independent record of votes that can be verified by the voter before casting the ballot. VVPAT is one of a class of security methods called independent dual verification (IDV).[32] These methods have in common the creation of two truly independent records of the voter's choices that the voter can verify and that can be compared in any audit.[33] Another IDV method, audio recordings of ballot choices, may be more voter-friendly than paper and exhibit superior verifiability.[34]

The above methods do not provide true voter verifiability, because the voter can verify the ballot only before it is cast. A third method uses cryptographic techniques[35] to allow the voter to verify *after casting the ballot* that it was counted correctly, without violating ballot secrecy.[36] It also permits voters to verify that no ballots were changed, added, or subtracted inappropriately — a feature known as results verifiability. Thus, this method could potentially make the election process far more transparent than is possible with other approaches.

Methods could also be developed that do not require the voter to separately verify the choices made on the DRE. Conceptually, this approach would be equivalent to taking a separate snapshot of the ballot choices listed on the face of the DRE just before the voter casts the ballot.

Security methods other than an independent ballot record might also provide ways to sufficiently manage any risks. For example, product standards for secure computing, such as the Common Criteria,[37] could be combined with sufficiently stringent engineering and administrative security practices to improve resistance to tampering.

---

[32] See Election Assistance Commission, "Independent Dual Verification Systems," *Voluntary Voting System Guidelines, Vol. 1, Appendix D,* draft, June 24, 2005, available at [http://guidelines.kennesaw.edu/vvsg/intro.asp].

[33] Most DREs record three separate electronic records of the voter's choices, but they are not independent of each other. They are simply separate recordings of a single event — the choices generated by the DRE when the voter casts the ballot. IDV systems would add another, separately verified record, usually but not necessarily involving another medium such as paper or audio.

[34] Sharon B. Cohen, "Auditing Technology for Electronic Voting Machines," Masters Thesis, Massachusetts Institute of Technology, May 19, 2005, available at [http://www.vote.caltech.edu/media/documents/draft%20a.pdf].

[35] The cryptographic technique of authentication permits a person who receives encrypted information to verify that the information is authentic — that it is legitimate and has not been altered in any way. This may be paired with techniques to assure confidentiality — that the recipient cannot read the information but only verify that it is authentic. One nonelectronic analogy is the use of a secure envelope that shows evidence of any tampering and is extremely difficult to counterfeit.

[36] The method is called "end-to-end (cryptographic) IDV" in the draft EAC guidelines.

[37] See CRS Report RL32777, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options,* by Eric A. Fischer, for more detail.

Does a VVPAT ensure that a voter knows how votes were recorded on a DRE? One consequence of the secret ballot is that a voter cannot know how his or her vote is recorded, unless certain cryptographic techniques are used. With VVPAT, a voter is given the opportunity, before the vote is cast, to review a paper printout of ballot choices made and to compare them to the choices listed on the DRE display. If the voter finds a discrepancy, the ballot can be cancelled and a new voting session begun. However, once the ballot is cast, the voter does not know what was actually recorded in the DRE's memory. Any discrepancies between the recorded vote and the printout can be discovered only by election officials if they compare the electronic and printed records after the election. The circumstances under which they would do that will depend on state and local election law and procedures.

True voter verifiability, in which the voter can confirm that the ballot was counted as intended, is possible without violating ballot secrecy, but is not currently in use in U.S. federal elections. The simplest way to achieve verifiability is to have ballots publicly counted and associated with the names of the voters — analogous to a recorded vote in the House or Senate. A classic example in public elections would be voice voting for candidates in a town-hall meeting. However, such methods would eliminate ballot secrecy, which is generally regarded as an important safeguard against voter fraud and coercion. Other methods, though, could be used that do not compromise ballot secrecy. For example, cryptographic techniques used in national security permit a secret message to be authenticated without revealing its contents. Similarly, they can provide voters the ability to determine that their ballots were counted accurately without revealing the actual votes cast (see above). Some systems using this approach have been developed.[38]

Are paper-based ballots the most secure? There appears to be an assumption among many VVPAT advocates that paper ballots are far more secure and less subject to fraud and tampering than are DREs, but whether that is so has not been established as fact. It is generally accepted that paper has certain desirable security features compared to electronic records — for example, it is durable; it can be difficult to alter without detection; and it can be directly inspected without the use of machines or devices.[39] However, paper also has several security weaknesses in comparison — for example, it is easy to manipulate by hand without specialized tools; it does not eliminate risk from Trojan horses or other malware if counting is done with the aid of computers; and, unlike electronic records, it cannot take full advantage of the protections afforded through the use of cryptographic techniques, although those techniques are not currently used in public elections in the United States.[40]

---

[38] Ibid.

[39] This point has been made by several security experts in different public fora, perhaps most notably David Jefferson, a computer scientist at Lawrence Livermore National Laboratory who chaired the California Secretary of State's Task Force on Internet Voting.

[40] David Jefferson, "Internet Voting," PowerPoint presentation, April 4, 2001, available at [http://www.hss.caltech.edu/~voting]. However, Jefferson subsequently became a supporter of VVPAT.

The evolution of voting security can be considered a kind of arms race, with new technologies developed to combat fraud, and miscreants evolving ways to attack each new technology in turn. For example, the bribery associated with voice voting in the eighteenth and early nineteenth centuries was countered by the use of paper ballots, which evolved into ticket ballots provided by the political parties. Subsequently, the Australian secret ballot was adopted to combat the fraud that became associated with the ticket ballot, and the lever machine came into wide use in part because it prevented certain kinds of fraud that had become prevalent even with the Australian ballot.[41] For example, lever machines and DREs prevent a particularly notorious kind of ballot fraud known as chain voting, in which each voter obtains a previously marked ballot before entering the poll, deposits that ballot, and leaves with the unmarked ballot the voter obtained in the polling place. That ballot is then marked for the next voter. Other classic forms of ballot fraud with paper ballots include such methods as stuffing of the ballot box, altering or substituting ballots, and producing fraudulent counts.[42] At least some of these methods can be made more difficult with the proper use of voting technology, including lever machines, DREs, and counting devices, although all of those systems have potential vulnerabilities of their own. In addition, recent technological advances have made production of counterfeit ballots and other methods for tampering with paper ballots potentially more feasible.[43]

The arms-race characteristics of the evolution of voting systems strongly suggests that VVPAT would have exploitable vulnerabilities that might not yet be apparent.[44] For that and other reasons, a simple reliance on such a technological solution, or any "magic bullet" countermeasure, is unlikely to be successful. In general, effective security uses a layered, multifaceted approach that involves procedural and technological safeguards as well as technology.[45]

Are paper ballots essential to ensure transparency in an election?
There is not a generally agreed definition of transparency in the context of elections. However, it is usually taken to mean that election processes are open and observable

---

[41] Joseph P. Harris, *Election Administration in the United States* (Washington, DC: The Brookings Institution, 1934), p. 1 — 20, 57 — 60, 261 — 264.

[42] See, for example, ibid., p. 315 — 382. There do not appear to be any recent comprehensive studies of ballot fraud (see Lori Minnite and David Callahan, *Securing the Vote: An Analysis of Election Fraud,* report, April 14, 2003, available at [http://www.demos-usa.org/pub111.cfm]); however, at least one recent book has compiled various cases and allegations (see John Fund, *Stealing Elections: How Voter Fraud Threatens Our Democracy*, (San Francisco: Encounter Books, 2004).

[43] Douglas W. Jones, "Chain Voting," paper submitted for the workshop, "Developing an Analysis of Threats to Voting Systems," National Institute of Standards and Technology, October 7, 2005, available at [http://vote.nist.gov/threats/papers/ChainVoting.pdf].

[44] For descriptions of some possible threats, see National Institute of Standards and Technology, "Threat Analyses & Papers," October 21, 2005, [http://vote.nist.gov/threats/papers.htm].

[45] See CRS Report RL32139, *Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues*, and CRS Report RL32777, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, both by Eric A. Fischer, for more detail.

in all of their essential parts, so that tampering, malfeasance, incompetence, and other threats to integrity are difficult to hide. Voter verifiability is arguably an important component of transparency, and to the extent that paper ballots provide verifiability, they can be important to transparency. However, as discussed in more detail above, the requirement for ballot secrecy as an anti-tampering measure severely limits the ability of paper ballots to provide verifiability, and other methods may prove superior when used with electronic voting systems. Consequently, paper ballots are not essential to ensure the transparency of an election.

Does VVPAT violate ballot secrecy? The secret ballot has long been recognized as important in the prevention of fraud and coercion in voting.[46] Some observers have misunderstood VVPAT as permitting voters to remove the printed list of ballot choices from the polling place, which would compromise ballot secrecy. However, that is not how this verification method works. As used in conjunction with DREs, VVPAT can be seen by the voter but not handled or removed from the polling place. As a result, they cannot be used by voters to prove how they voted.[47]

There is one way in which VVPAT can potentially compromise ballot secrecy. Most current implementations print the ballot choices on a roll of paper. If someone at the polling place keeps track of the order in which voters use a given DRE, it would be possible to identify which voter cast which ballot on that machine. However, there are several possible countermeasures for this vulnerability. In fact, the only voting method currently in use in federal elections for which violations of ballot secrecy is a significant potential concern is the absentee or mail-in ballot.

Do paper ballots pose only a minor inconvenience for persons with disabilities? Paper ballots have long posed problems for voters with disabilities, including blind voters, some voters with impaired sight, and voters with other types of disabilities that prevent them from filling out a paper ballot. In the past, a paper ballot could be filled out by a person designated to do so by a disabled voter, but the ballot was not secret, and blind voters had no means of verifying that their choices were properly marked. At a polling place, a disabled voter needed to bring someone with them or accept the assistance of someone at the polling place, often a stranger.

HAVA changed that arrangement by requiring that polling places provide at least one voting machine that is accessible to voters with disabilities and provides the same level of secrecy and verifiability as for other voters (§301(a)(3)). DREs outfitted with a paper audit trail cannot be verified at present by certain disabled voters, particularly blind and sight impaired voters. In a Senate Rules Committee hearing on voter verification in June 2005, Senator Christopher Dodd, a HAVA

---

[46] See, for example, Harris, *Election Administration*: "It appears that bribery was prevalent in the colonies without the secret ballot, and constituted in all probability the worst abuse in colonial elections" (p. 16).

[47] There is at least one exception: A voter could write in an agreed-to nonsensical name for a contest that is not of interest. A corrupt election official could then examine the ballot and identify that voter's choices in contests that are of interest. However, this method is possible for any consolidated ballot (it would not work with lever machines) and would seem impractical for almost all public elections.

cosponsor, noted, "We say in HAVA that every voter must have the right to verify their ballot before the ballot is cast…all of the legislation or most of it that has been introduced excludes the ability of the disabled to have the same right. By insisting on paper, we are denying the people who cannot read because they cannot see, or for reasons otherwise cannot manually operate the system, a chance to verify what they have done."[48] The accessibility problems with paper ballots are potentially solvable but would require the use of additional technology, such as electronic reading aids.

Is VVPAT a proven technology that is simple to implement? While the basic technology used in VVPAT is proven, the system as a whole is not, and there is currently no approved federal standard for this verification method. However, a draft standard is included in the VVSG currently under consideration by the EAC. VVPAT also adds a significant level of complexity to DRE voting, both because of the additional technology required and the effort needed by a voter to compare the on-screen and printed ballots. It also adds complexity to the administration of an election by requiring procedures for handling and processing paper ballots in addition to the electronic ballot records. There has been little testing of VVPAT in public elections.

Among the drawbacks of VVPAT cited by critics is the added cost to states (in addition to the cost of HAVA requirements), the lack of data on its performance, and problems associated with the technology in actual use. There were reports of jammed printers in some places in 2004,[49] but there are not enough data to assess any potential long-term problem with jamming. Whether a paper trail assists voters in correcting errors is unknown and probably difficult to measure. What little research is currently available suggests that voters do not use it effectively as it is currently implemented.[50]

Recounts and Audits

Is an audit of an election the same as a recount? An election recount is intended to confirm an election result, because a contest was particularly close or for some other reason that called the initial result into question. The focus of a recount is the voted ballot, rather than an examination of voting equipment or voting processes. Recounts and the methods for triggering them vary by state. Some states require an automatic (partial) recount for a close race; other reasons for conducting

---

[48] Statement of Senator Christopher J. Dodd, Senate Rules Committee hearing on voter verification in federal elections, June 21, 2005, available at [http://www.senate.gov/hearings/2005/062105_hearing.htm].

[49] Ted Selker, "Processes Can Improve Electronic Voting: A Case Study of an Election," Caltech/MIT Voting Technology Project, October 2004, available at [http://www.vote.caltech.edu/media/documents/vtp_wp17.pdf].

[50] See Ibid.; Sharon B. Cohen, "Auditing Technology for Electronic Voting Machines," Masters Thesis, Massachusetts Institute of Technology, May 19, 2005, available at [http://www.vote.caltech.edu/media/documents/draft%20a.pdf]; Paul S. Herrnson, "Beyond the Hanging Chad: The Promise and Performance of Electronic Voting," PowerPoint Presentation, University of Maryland, October 26, 2005, available at [http://www.capc.umd.edu/rpts/Beyond_the_Hanging_Chad.pdf].

a recount may include a demonstrated irregularity or other evidence that a result is questionable and may require a recount, or a formal request by a candidate.

An audit is an in-depth examination of the accuracy of the voting process as a whole, rather than just the voted ballots or election totals. With proper record-keeping, an audit can facilitate a step-by-step examination of how a voting machine recorded cast ballots and computed vote totals to determine whether it performed accurately. Audits may also review the chain of custody for voting equipment, printed ballots, registration lists (and the method of compiling them), deployment of voting equipment, and the vote-counting process. Presumably, an audit can examine any aspect of the election process that can be measured or recorded.

Some VVPAT proposals require that the paper print-out be the ballot of record in the event of any differences detected between the paper and electronic records. The basic argument in favor of the position is that the paper ballot is more trustworthy, since the voter had the opportunity to examine it directly. Others, however, point out that this approach may actually create vulnerabilities, since miscreants could simply focus their attacks on the paper ballots. They say it is preferable to use the entire audit trail to determine the correct outcome in the event of a discrepancy.

Will a partial recount determine if fraud occurred? Some VVPAT proposals include the requirement that hand recounts be done of a sample of the paper ballots and compared to the machine counts recorded by the DREs. The likelihood that such an approach will detect any irregularities depends on several factors. To be effective, a sample recount would need to provide for a meaningful comparison of recount results with original tallies. One way to do that is to recount entire precincts. The number recounted would need to be high enough to provide a reasonable probability that inaccuracies would be detected. That number will depend on the degree of inaccuracy election officials are interested in detecting,[51] as well as

---

[51] For example, if 5 out of 100 precincts reported results incorrectly, selecting and recounting only 1 out of the 100 precincts would fail to discover the problem 95% of the time. Recounting 13 precincts would be needed to lower the detection-failure probability to 50%. However, if 10% misreported, recounting only 7 would be needed to yield a failure probability below 50%, but 50 would need to be recounted if only 1 precinct misreported. Curiously, under this model the number of precincts that need to be recounted does not change greatly for a given misreporting rate as the total number of precincts increases. Thus, to detect a 1% misreporting rate with 50% probability among California's 25,000 precincts requires recounting only 69 precincts. The numbers are determined using a simple probability calculation analogous to that used to solve the "birthday problem" (what is the probability that at least two people in a group of a given size share the same birthday?). If there are 100 precincts, and five are reporting incorrectly, that means 95 of the precincts have no error. Then, assuming recounting will always detect any error in a given precinct (not realistic in practice), if a single precinct is chosen at random for a recount, the probability that the recount would be done on a precinct that reported correctly is 95 out of 100, or 95%. In that case, if a second precinct is counted, the probability that a correctly reporting one is chosen will be 94 out of the 99 remaining, or 94.9%. The probability that an incorrectly reporting precinct would be missed in both cases is obtained by multiplying the two probabilities: 95% * 94.9% = 90.9%. The process is repeated to determine

(continued...)

the probability of detection deemed necessary to serve as a sufficient deterrent to potential miscreants.

Are hand counts more accurate than machine counts? VVPAT proposals often stipulate that recounts of paper ballots must be done by hand. They often argue that only direct counting by humans can ensure accuracy. That may indeed be the case in some circumstances, but it is not likely to hold broadly. In general, humans are not as accurate as machines in performing simple, highly repetitive tasks such as counting ballots. They tend to make many more errors. That is one reason why repeated manual recounts may yield different results.

Machine accuracy is especially likely to be higher if the ballot choices made by the voter are printed, as they are with VVPAT. In contrast, machines are not as good at judging voter intent if markings are ambiguous or not within machine parameters, as may be the case if the ballots are marked directly by voters, as in optical scan systems. Machine miscounts can also result from miscalibration or other technical failure, or potentially from malware if it has been implanted. However, there are several ways to guard against such problems.

Possible Issues for Congress

As of December 2005, at least 25 states require paper ballot records, and at least 14 more are considering such a requirement.[52] However, neither Maryland nor Georgia, which use DREs statewide, enacted such requirements, opting instead to focus on other security approaches. With the exception of Nevada, no state has used VVPAT statewide in a federal election. As the technology is used by more states in the future, more will be known about the cost, performance, and any limitations of VVPAT in normal use. Misperceptions about DREs could have important policy implications as states, and possibly Congress, consider proposals to require VVPAT for all electronic voting machines. In particular, the following issues may be worth considering:

Lack of information. There remains considerable uncertainty about the relative security of DREs in comparison to other voting systems; how security measures such as VVPAT may impact other important goals such as accuracy, reliability, usability, and accessibility; and the effectiveness of those security measures. Congress could direct the EAC to fill those information gaps through appropriate research as states move to implement VVPAT and other security measures.

Potential conflicts with HAVA requirements. To the extent that states require paper-based ballots, they may be perceived to be in violation of the accessibility

---

[51] (...continued)
probabilities associated with adding additional precincts. See also C. Andrew Neff, "Election Confidence: Comparison of Methodologies and Their Relative Effectiveness at Achieving It", December 17, 2003, available at [http://www.votehere.net/papers/ElectionConfidence.pdf].

[52] Election Reform Information Project, *Voter-Verified Paper Audit Trail Legislation & Information*, available at [http://www.electionline.org/Default.aspx?tabid=2890].

requirements of HAVA, unless their paper-based systems can be made sufficiently accessible. Congress might be asked to resolve any such conflicts through changes to HAVA.

Voter Confidence. One of the arguments used in favor of VVPAT by some observers is that it is necessary to help restore voter confidence in the U.S. election process.[53] However, there is little evidence that confidence of the average voter is affected by this issue.[54] Even if the adoption of VVPAT does increase confidence in the electoral process, if that confidence is false — as might be the case if voters mistakenly believe that a paper-ballot requirement is a "magic bullet" security measure — that could itself pose a risk to the integrity of elections. Congress may wish to examine the extent and causes of any decline in voter confidence, and the impact of various possible measures on it, in considering whether to enact legislation relating to this matter.

Impacts on Innovation. While the mandating of security requirements such as VVPAT can result in innovation with respect to those requirements, there is a risk that the requirements will be written in such a way that other kinds of innovation, such as potentially superior security measures not using VVPAT, will be difficult to implement without additional legislation. Congress may wish to consider ways to ensure that the federal and state regulatory environment for voting systems does not inhibit such innovation.

---

[53] This point was made, for example, by the Carter-Baker Commission [http://www.american.edu/ia/cfer/] as one of the reasons for its recommendation that paper ballot records be required.

[54] See, for example, Herrnson, "Beyond the Hanging Chad."