Letter Report on Electronic Voting

Committee on a Framework For Understanding Electronic Voting, National Research Council

ISBN: 0-309-66339-3, 12 pages, 8 1/2 x 11, (2006)

THE NATIONAL ACADEMIES
Advisers to the Nation on Science, Engineering, and Medicine

Computer Science and Telecommunications Board

500 Fifth Street, NW
Washington, DC 20001
Phone: 202 334 2605
Fax: 202 334 2318
E-mail: cstb@nas.edu
www.cstb.org

July 20, 2006

Lawrence Brandt
Program Director
Information Integration & Informatics (III) Cluster
Directorate for Computer and Information Sciences and Engineering
National Science Foundation
4201 Wilson Boulevard
Arlington, Virginia 22230

Dear Dr. Brandt:

With this letter report,[1] the National Research Council's Committee on a Framework for Understanding Electronic Voting (Appendix A) seeks to provide some idea of the current state of readiness for electronic voting in jurisdictions across the United States and to gauge what progress has been made since the publication of the committee's 2005 report, *Asking the Right Questions About Electronic Voting*.[2] This second report of the committee is based on a May 2006 workshop that brought together a number of knowledgeable and thoughtful local, state, and federal election officials (Appendix B) who shared their perspectives and experiences with the committee.[3] Presentations and discussions at the workshop made clear that many of the issues

---

[1] The preparation of this letter report was supported under National Science Foundation Award Number IIS-0436133. However, in accordance with National Research Council policy, the NSF did not review this report before publication, and the opinions, findings, conclusions, or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the NSF.

[2] For more information, see National Research Council, *Asking the Right Questions About Electronic Voting*, The National Academies Press, Washington, D.C., 2005. See also http://www.cstb.org/pub_evoting.html.

[3] The analysis, conclusions, and recommendations presented in this letter report are the responsibility of the committee alone and should not be attributed to these officials or anyone else. Furthermore, the justification for the committee's conclusions and recommendations does not lie in a statistically valid sampling of the nation's voting jurisdictions but is instead based on a mix of inputs. Testimony to the committee by the officials listed in Appendix B was intended to put a human and contemporary face on the nature of difficulties that jurisdictions are likely to face if problems arise in conducting the November 2006 elections.

discussed in *Asking the Right Questions* remain open and quite fluid as the nation approaches the 2006 elections—these issues include reliability, usability, security, training, education, and testing/certification.

The scope of this letter report is restricted to readiness for using electronic voting systems, by which is meant the systems with which voters interact directly to cast their ballots. Direct recording electronic (DRE) systems are the most obvious example, but electronic voting systems also include optical scan systems. In these latter systems, the voter marks his or her preferences on a physical paper ballot; the ballot is then read by an optical scanner, and the vote is passed to a tabulation mechanism for counting. This report is concerned primarily with readiness for the November 2006 elections, rather than with longer-term issues. For a discussion of longer-term issues, the reader is advised to consult *Asking the Right Questions*.

CURRENT STATUS OF PREPARATION FOR THE NOVEMBER 2006 ELECTIONS

On the basis of the testimony of the local, state, and federal election officials present at the workshop, the expertise developed by the committee in preparing its September 2005 report, and the experience and background of individual committee members, the committee believes that some jurisdictions—and possibly many—may not be well prepared for the arrival of the November 2006 elections with respect to the deployment and use of electronic voting equipment and related technology, and anxiety about this state of affairs among election officials is evident in a number of jurisdictions. Several factors appear to contribute to this unease and concern:

- *Compliance deadlines tied to the November 2006 elections that are required by the Help America Vote Act (HAVA)*. Some states and jurisdictions have failed to meet HAVA-mandated deadlines already, and others are likely to miss deadlines tied to the November 2006 election (and thus will carry out the fall elections with equipment and systems that are not HAVA-compliant), although it remains to be seen what legal or political consequences, if any, will flow from these missed deadlines. Other jurisdictions will meet HAVA deadlines in a technical sense but may not be able to fulfill certain key HAVA objectives, such as increasing voting booth accessibility for disabled voters or reducing the error rate in the ballots cast.[4] In still other cases, jurisdictions rushing to meet deadlines for HAVA compliance might have done so in counterproductive ways, such as by buying equipment that is not up to par, using software that may not be fully compatible with existing applications, not becoming sufficiently familiar with vendor products, and so on.
- *State legislative activity*. Entirely apart from HAVA, many states have imposed additional requirements for election equipment and have set new requirements for election procedures. For example, at least 26 states have passed laws mandating that voter-verified paper audit trails (VVPATs) be provided for voting

[4] Issues related to reducing voter error rates are discussed in *Asking the Right Questions*, pp. 82-95.

equipment that will be used in the November elections.[5] For some of the states that are using retrofitted DRE systems, the 2006 primary election represents the first large-scale use of VVPAT-equipped voting systems.[6] That is, the concept of voter verification of votes cast on DRE systems has never been tested on a large scale in any U.S. election, and the impact of this particular capability on election results and public confidence in them has yet to be seen.

- *Security*. Security issues remain prominent in the public debate about voting technologies.[7] For example, even as the committee was meeting, concerns were spreading about a new vulnerability discovered in one prominent vendor's equipment.[8] On June 27, 2006, New York University's Brennan Center for Justice released a report focusing on security vulnerabilities in electronic voting machines.[9] Physical security was also discussed at the workshop—with one official recounting the difficulties in providing adequate warehousing space for her e-voting equipment, as well as concerns about how to transport such equipment safely and securely.
- *Vendor performance*. Several workshop participants in contractual relationships with two prominent vendors reported on nontrivial problems with poorly designed, poorly tested, or poorly constructed e-voting equipment. For example, equipment has been delivered with many sample defects, including such things as sharp edges on machines and broken legs on machine stands. In other cases, some vendors are meeting promises regarding delivery of equipment by supplying for shared use equipment that has been used in other jurisdictions. Such sharing has been possible when (primary) elections are held on different dates, but this tactic obviously cannot be used on November 7, 2006.
- *Poll worker availability*.[10] In some jurisdictions, the availability of trained poll workers may be an issue in the fall. Some election officials at the workshop

---

[5] See, for example, http://www.verifiedvoting.org.

[6] A modern DRE system usually has a screen that displays the ballot to voters. For accepting input, some have touch screens, while others use mechanical selection devices. When the voter is finished voting, the voter takes some action in front of the machine to finalize his or her ballot. When a VVPAT is attached to the system, the voter has the opportunity to view a paper record of his or her vote that is then stored with the system just before the finalization action is taken. See *Asking the Right Questions*, pp. 39-42.

[7] For more discussion of security issues, see *Asking the Right Questions*, pp. 57-82.

[8] See Monica Davey, "New Fears of Security Risks in Electronic Voting Systems," *New York Times*, May 12, 2006. Available at http://www.nytimes.com/2006/05/12/us/12vote.html?ex=1305086400&en=5b3554a76aad524a&ei=5090&partner=rssuserland&emc=rss.

[9] Brennan Center Task Force on Voting System Security, *The Machinery of Democracy: Protecting Elections in an Electronic World*, Brennan Center, New York University, New York, 2006. Available at http://www.brennancenter.org/programs/downloads/Full%20Report.pdf.

[10] See *Asking the Right Questions*, pp. 100-105.

reported concerns that they will not be able to train enough poll workers in how to use the new equipment for November, a prospect that they believe will result in very long lines, excessive delays, and voter confusion if poll workers are unable to answer questions about the new systems. Poll workers must be trained in system setup and basic troubleshooting, as well as in answering questions that voters are likely to have—and even poll workers with experience from past elections may not be of much assistance to voters if they themselves are unfamiliar with the electronic voting systems at their polling places.

- *Voter education*.[11] For many voters, the November 2006 election will be the first conducted with electronic voting systems. Election officials are concerned about voter readiness to use these new technologies, as well as the related question of citizen confidence in the newly deployed systems.

This set of observations is not intended to suggest that all jurisdictions are facing these issues with the same concern and intensity. Indeed, perhaps the committee's most salient impression as the nation approaches the fall elections is the wide variation in the situations of the various jurisdictions, the consequences and implications of which remain to be seen.

EMERGING FACTORS AND REALIZATIONS

As jurisdictions proceed along the path toward electronic voting in November 2006, a number of factors are becoming more apparent.

First, jurisdictions are becoming more aware of the cost implications of deploying electronic voting systems, in particular, the fact that the initial acquisition cost of an electronic voting system is only a fraction of the total life-cycle cost.[12] Furthermore, HAVA appropriations represent a one-time infusion of federal money to the states (most of which has already been spent on equipment purchases),[13] and no supplemental funds are likely to be forthcoming from either the federal government or the states for conducting elections. Thus, many jurisdictions are facing the November elections without adequate financial resources to address the problems they see on the horizon—problems including equipment testing; maintenance and storage; training of poll workers; and voter education.

A second factor is that as some jurisdictions have learned for themselves about the complexities of electronic voting, their relationships with e-voting equipment vendors and service providers have become increasingly adversarial. For example, a number of workshop participants reported that they have become more assertive in their dealings with vendors and are less willing to accept what they believe to be shoddy work or broken promises: some reported having developed more leverage and expertise in negotiating contracts and terms with vendors. But other workshop participants reported having problems with and less success in obtaining desirable provisions for contracts

[11] See *Asking the Right Questions*, pp. 93-95.
[12] See *Asking the Right Questions*, p. 97.
[13] See *Asking the Right Questions*, p. 114.

they were negotiating. Also, some workshop participants reported that colleagues from smaller jurisdictions with fewer resources, and perhaps lacking the necessary legal, technical, or contracting expertise to negotiate more favorable terms, simply accept the standard vendor contract.[14]

Third, election officials are increasingly realizing the fundamental contradictions between relying on current procedures and requirements for certifying voting system software,[15] on the one hand, and holding elections on fixed, immovable dates, on the other.[16] The fundamental reality of software is that problems can emerge after the software has been certified and put into use, and some of these problems may be serious enough to require fixing. However, ensuring that the installation of a fix does not have other, unintended consequences (e.g., causing yet another problem) can be a difficult process, and re-certification of modified software can be quite time-consuming. Yet elections are held on the first Tuesday of November and are postponed only under extraordinary and rare circumstances—and it is unlikely that the lack of certification for a patched software system would be regarded by election officials as such an extraordinary circumstance. Thus, in the event that problems are found after certification, election officials must then choose between using certified systems with known problems or using uncertified systems in which those problems may have been fixed—and the latter may be regarded by some election officials as the lesser of two evils.

A fourth factor is the extent and scope of vendor involvement apart from the sale of equipment itself.[17] For example:

- Workshop participants expressed considerable skepticism about current certification processes for electronic voting systems,[18] given the lack of an arms-length relationship between the independent testing authorities (ITAs) and the vendors. Rightly or wrongly, these concerns originate in the fact that vendors pay the ITAs for undertaking certification.[19] In addition, vendors have opportunities to tune their software specifically for the tests in question, a practice somewhat akin to studying for a test rather than learning the material in a course. Lack of certification reform has also contributed to such skepticism.

---

[14] The group of election officials assembled for this workshop agreed that their jurisdictions have relatively greater access to resources than do most other jurisdictions and thus are not necessarily representative of most jurisdictions across the nation. The committee also noted that most voting jurisdictions in the nation are on the smaller side.

[15] Note that software is used in electronic ballot marking systems and electronic tabulation systems, and both generally require certification.

[16] See *Asking the Right Questions*, pp. 110-114.

[17] See *Asking the Right Questions*, pp. 120-122.

[18] See *Asking the Right Questions*, pp. 110-114.

[19] The mere fact that a vendor pays for a testing procedure should not itself be damning. For example, Underwriters Laboratory has provided product certification for many years. Although product manufacturers pay for the testing and certification process, UL certification has some notable credibility in the marketplace.

- In some cases (involving both DRE and optical scan systems), vendors are responsible for generating the various vote counts that emerge from an election—a function that has traditionally and historically been an inherently governmental function. Although election officials continue to have ultimate responsibility for the integrity of an election even when privatized vote counting is in place, vendors with profit-making motives have high incentives to cut corners and to refrain from incurring costs in resolving disputed votes.
- Electronic voting equipment is complex and thus requires considerably more training to operate (especially with respect to troubleshooting issues). Vendors are thus necessarily involved in training efforts for election personnel and poll workers.

Fifth, several workshop participants commented on the incompleteness of testing of electronic voting equipment by vendors and ITAs, which—by assumption—do not address needs or issues that are specifically local. For example, paper trails attached to voting systems must be generated by a printer. Often these printers use thermal paper—but voting records printed on thermal paper may not last as long as is required by local law. Some officials at the workshop noted that they would have preferred to undertake their own testing but that resource constraints (money, personnel, and time) prevented them from doing so. Given the complexity of systems, the quantity of patches, and the variety of ballot positions and configurations to test, it is not clear that electronic voting machines can be adequately tested before being deployed.

Sixth, election jurisdictions vary widely in their knowledge and expertise regarding electronic voting.[20] Those with less knowledge about technology or with less experience in contracting with technology vendors clearly operate at a disadvantage in preparing for the November elections, and a lack of technology background or contracting experience regarding assessments of quality, performance, and reliability can increase the influence of politics and personal relationships in the procurement process. Election officials in such jurisdictions could benefit from their more experienced colleagues in learning about problems associated with the products of different vendors, solutions to such problems, jurisdiction-appropriate contract provisions, backup procedures and contingency plans, and law and regulation. In addition, it is simply a fact that, viewed in the large, electronic voting systems are a relatively new arrival on the election scene, and few jurisdictions can claim to have a great deal of experience with such systems.

Finally, advocacy groups have gained considerable influence in the debate regarding electronic voting. Many of these groups focus on security issues[21] and play an increasingly important role in focusing public attention on the conduct of elections and in stimulating state legislative action intended to mitigate security risks.

[20] See *Asking the Right Questions*, p. 118.

[21] For a more extended discussion of security issues raised by some advocacy groups, see *Asking the Right Questions*, pp. 57-82.

RECOMMENDATIONS

As the November 2006 elections approach, the committee's first and most urgent recommendation is that **election jurisdictions should—indeed must—ensure the availability of backup mechanisms and procedures for use in the event of any failure of e-voting equipment or related technology.** This recommendation is based on the fact that any "flash" cutover to new technology (such as we are seeing today with many e-voting systems) almost guarantees surprises and unintended consequences (e.g., system crashes, unacceptably slow performance). And, although unlikely if appropriate pre-election testing has been undertaken, election officials would be unwise to completely ignore the possibility of problems severe enough to prevent the effective use of the entire system for some period of time on Election Day.

Most organizations have learned the hard way that it is necessary to develop, test, evaluate, and iterate with small-scale prototypes before committing themselves to an organization-wide program of technology upgrade. They have also learned that they should plan on the simultaneous availability of both old and new systems for some period of time, so that failures in the new system do not leave them unable to perform their mission.

Mostly as the result of resource constraints, most election jurisdictions are not (and have not been) in a position to ask vendors for small-scale testing of prototypes in an operational environment before committing to large-scale deployment. Accordingly, jurisdictions must have backup and contingency plans in place that anticipate a wide range of failure conditions, including failures in the middle of the voting process on the day or days of voting.

The committee does not make a specific recommendation on the precise nature of the appropriate backup plans, as these will vary from jurisdiction to jurisdiction. Moreover, there are budgetary constraints on the comprehensiveness of any contingency plan that can be put into place—jurisdictions may only be able to plan for relatively modest problems, such as local system failures in individual precincts, rather than for widespread failures on Election Day.

For risks to system operation involving individual polling places, one option might be for all precincts to have available the location of a number of other precincts to which voters might be redirected. Another option might be to have available and on call technicians and/or a few spare voting machines in a van that could be redeployed promptly. A third option is to ensure that a reasonable stock of hand-countable paper ballots is created before the election and designated for use only in an emergency that renders the original voting method unusable. With preprinting of such ballots, election administrators would have a much easier time accounting for any hand-countable ballots that were produced and/or used.[22] Counting paper ballots is discussed in Appendix C.

---

[22] Still another alternative is to create paper ballots on short notice by making arrangements with a printing firm to use special-purpose ballot stock paper, which would make ballots easier to reconcile as compared to regular stock. Rush jobs to print ballots on Election Day are subject to many potential difficulties, however, such as the drying time for the ink used to print ballots. To the extent that emergency ballots can be created ahead of time without the pressure of immediate (same-day) delivery, many

To prepare for the possibility of widespread failures (i.e., voting systems made inoperable on a large scale, whether by technology or acts of nature), election officials need to engage in a contingency planning process focused on such a possibility.[23] Almost certainly, the choices would be choices among bad alternatives, each one disenfranchising voters to some extent. Primaries and elections for local offices, at least, have been postponed following external disasters, as was done in New Orleans in the aftermath of Hurricane Katrina and in New York City following the 9/11 attacks on the World Trade Center.

Apart from this primary and urgent recommendation, the committee urges that to the extent possible, **jurisdictions should band together in their interactions with vendors.** With 9,500 election jurisdictions in the nation and only a handful of major electronic voting system vendors, it is clear that the leverage of jurisdictions vis-à-vis vendors would be increased significantly if they could present their requirements collectively, for example as part of a negotiating consortium. Even if not, informal information sharing (e.g., about what a vendor is willing to do for one jurisdiction) can support efforts at moral suasion to persuade vendors to be more accommodating to jurisdictions' needs.

Election officials should also seek information from their colleagues about problems associated with the products of different vendors, solutions to such problems, jurisdiction-appropriate contract provisions, backup procedures and contingency plans, and legal and regulatory options. Since jurisdictions are generally not in a position to undertake such research themselves, they might request such assistance from the Election Assistance Commission and other entities in developing a national clearinghouse and resource for information regarding election administration. For example, these organizations could compile best practices related to contracting with vendors for e-voting equipment and related services, develop a database of state election laws to facilitate easy comparisons and information exchange, and establish discussion forums for election officials in which problems and solutions could be discussed candidly.

Finally, **jurisdictions should consider engaging in parallel testing of their voting systems on Election Day if it is feasible to do so.** In parallel testing, some

---

such problems can be avoided.

[23] A few examples can be cited of contingency/threat planning related to elections and elected bodies. For example, Dana Debeauvoir, from Travis County, Texas, produced a report about a planning process that was honored by the Election Center in 2005 (the package of papers is at http://electionupdates.caltech.edu/2005/12/election-center-2005-professional.html). A second example is provided by Oregon, whose state election code requires that each county election official file an elections security plan annually with the Secretary of State. The plan is supposed to include a presentation of security procedures. Third, the Continuity of Government Commission has addressed the issue of ensuring that the Congress could reconstitute itself quickly in the aftermath of a large-scale terrorist attack that killed or incapacitated a large number of senators and/or representatives (see http://www.continuityofgovernment.org/report/report.html). However, none of these efforts specifically address the question of contingency planning for Election Day mishaps.

randomly chosen systems are taken out of service and used instead in a simulated, videotaped "election." Pre-scripted votes are entered as they would be if the machines were in actual use, but since these votes are known, the final vote counts can be checked for accuracy. The committee understands that many jurisdictions will not be able to undertake parallel testing in November 2006 because of time and resource constraints, but to the extent that such testing can occur, it would help to inform others for the 2008 election, and if successful, might help bolster confidence in it as well.[24] This recommendation holds for all jurisdictions that do not use hand-counted paper ballots, but it is particularly important for jurisdictions that use DRE systems not equipped to generate paper trails.

CONCLUSION

Throughout its deliberations and meetings since the start of this study in 2004, the committee has been struck by the dedication and talent of the election officials who have testified. Indeed, these individuals can be regarded as unsung heroes who have kept the machinery of American democracy operating in the face of sometimes overwhelming difficulties. But the November 2006 elections pose challenges like no other previous one regarding reliability, usability, security, training, education, and testing. More jurisdictions than ever before will have electronic voting systems in their polling places. Most importantly, the waiver available for the November 2004 election and provided by HAVA—which allowed states accepting funds for replacing punch card and lever voting systems to postpone replacement until January 1, 2006—has expired. In addition, the November elections appear at this point to be very close, and control of the House or Senate might rest on the outcome of a few close races whose results could be disputed.

However, these observations are not meant to suggest that there will be widespread failures of electronic voting systems, that election results will be clouded by excessive voter confusion about using new electronic voting systems, or that electronic election fraud will necessarily occur in November. Nevertheless, the circumstances of the November election raise the stakes for conducting elections that are regarded as fair and that can withstand close scrutiny even in the face of unproven technology and new election procedures. The challenges facing election officials and the nation in the upcoming election are formidable indeed, and only time will tell if election officials across the land will be able to succeed in the face of these challenges.

Respectfully submitted,

Dick Thornburgh and Richard Celeste, *Co-chairs*
Committee on a Framework for Understanding Electronic Voting

[24] For some additional discussion on parallel testing, see *Asking the Right Questions*, pp. 78-79. Note also that parallel testing itself must be undertaken carefully in order to minimize the possibility that test votes and real votes might be mistakenly intermingled.

APPENDIX A

MEMBERS OF THE COMMITTEE ON

A FRAMEWORK FOR UNDERSTANDING ELECTRONIC VOTING

DICK THORNBURGH, Kirkpatrick & Lockhart Nicholson Graham, LLP, *Co-chair*
RICHARD CELESTE, President, Colorado College, *Co-chair*
R. MICHAEL ALVAREZ, California Institute of Technology
THOMAS SHERIDAN, Massachusetts Institute of Technology (retired)
JOSEPH A. SMIALOWSKI, Freddie Mac
ANTHONY STEVENS, State of New Hampshire
PETER WEINBERGER, Google Inc.

Staff

HERBERT S. LIN, Senior Scientist and Study Director
KRISTEN BATCH, Research Associate
DAVID PADGHAM, Associate Staff Officer
BRANDYE WILLIAMS, Staff Assistant

APPENDIX B

LIST OF PARTICIPANTS IN THE MAY 12, 2006, WORKSHOP OF THE COMMITTEE ON A FRAMEWORK FOR UNDERSTANDING ELECTRONIC VOTING

Doug Chapin, Electionline.org
Donetta Davidson, U.S. Election Assistance Commission
Scott Doyle, Larimer County, Colorado
Eric Fischer, U.S. Congressional Research Service
George Gilbert, Guilford County, North Carolina
Gracia Hillman, U.S. Election Assistance Commission
Susan Inman, Pulaski County, Arkansas
Linda Lamone, Maryland State Board of Elections
Ray Martinez, U.S. Election Assistance Commission
Conny McCormack, Los Angeles County, California
Wendy Noren, Boone County, Missouri
Rene Peralta, National Institute of Standards and Technology
Ion Sancho, Leon County, Florida

APPENDIX C

ON THE MANUAL COUNTING OF PAPER BALLOTS

Counting paper ballots is inherently manual, but there are better and worse ways of doing it. One common method is based on ballot reading and tally marks. One member of a two-person team reads the ballot, declaring those legal votes apparent from the voter's marks. The second team member places a mark on his/her tally sheet for the candidate receiving a vote. This method involves the possibility of a mistake because the ballot is examined only once or a mistake because only one person is doing the tallying. Since this method commonly involves reading through the entire ballot, the ballot reader's eye and brain are not focused on looking for a single type of data, and thus the reader must expend mental effort to distinguish among the contests in which choices are made.

At least one state (New Hampshire), in its state recounts, has been using another process that seems to be less subject to error. This process, based on the use of ballot sorting and piles, involves one member of a two-person team picking up the ballots and placing them in piles corresponding to each choice in a particular race. The other team member observes each ballot as it is placed in a pile. After the sorting process is complete, one team member counts each pile in stacks of 25 and then the other team member recounts each stack. This process enables at least two persons to simultaneously examine each ballot at least once, and to keep things simple by identifying choices in a single race at a time. If one person makes a mistake, the other can catch it. This method is often modified so that each ballot is rechecked during the stack-counting process. Hence, each ballot can be seen two times by each member of the team, for a total of up to four views of each mark on a ballot in each race. The ballot sorting and pile method, which involves as many examinations of the same ballot as there are contests, is noticeably faster than the ballot reading and tally mark approach.