WRITTEN TESTIMONY OF DAVID WAGNER, PH.D.
COMPUTER SCIENCE DIVISION
UNIVERSITY OF CALIFORNIA, BERKELEY
BEFORE THE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES
U.S. HOUSE OF REPRESENTATIVES
MAY 7, 2007

Chairman Clay, Ranking Member Turner, committee members, thank you for the opportunity to testify today. My name is David Wagner. I am an associate professor of computer science at U.C. Berkeley. My area of expertise is in computer security and the security of electronic voting. I have an A.B. (1995, Mathematics) from Princeton University and a Ph.D. (2000, Computer Science) from U.C. Berkeley. I have published two books and over 90 peer-reviewed scientific papers. In past work, I have analyzed the security of cellphones, web browsers, wireless networks, and other kinds of widely used information technology. I am a member of the ACCURATE center, a multi-institution, interdisciplinary academic research project funded by the National Science Foundation[1] to conduct novel scientific research on improving election technology. I am a member of the California Secretary of State's Voting Systems Technology Assessment Advisory Board and of the Election Assistance Commission's Technical Guidelines Development Committee (TGDC)[2]. I have served as a poll worker in my county, and I served as a technical advisor to my county's equipment selection committee.

Summary

We have seen dramatic changes in election technology over the past decade. This new technology was introduced for laudable reasons and has brought important benefits. However, it has come at a cost.

Many of today's electronic voting machines have security problems. The ones at greatest risk are the paperless DRE voting machines. These paperless machines are vulnerable to attack: a single person with insider access and some technical knowledge could switch votes, perhaps undetected, and potentially swing an election. With this technology, we cannot be certain that our elections have not been corrupted.

In my research into electronic voting, I have come to the conclusion that the federal certification process is not adequate. The testing labs are failing to weed out insecure and unreliable voting systems. The federal certification process has approved systems that have lost thousands of votes, systems with reliability problems, and systems with serious security vulnerabilities. Over the past four years, independent researchers have discovered security vulnerabilities in voting machines used throughout the country—vulnerabilities that were not detected by state and federal certification processes. Unfortunately, the standards and certification process has not kept pace with the advances in election technology over the past decade.

In this testimony, I outline a number of potential directions for improving the federal certification process. I am encouraged by progress that has been made at the federal and state level, though I believe that there is more to do.

[1]This work was supported by the National Science Foundation under Grant No. CNS-052431 (ACCURATE). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

[2]I do not speak for UC Berkeley, ACCURATE, the California Secretary of State, the EAC, the TGDC, or any other organization. Affiliations are provided for identification purposes only.

One of the most promising directions may be to reduce our reliance upon software. With today's paperless voting machines, flaws in the software can potentially cause undetectable errors in the outcome of the election. That places an impossible burden on vendors and testing labs, because it requires perfection: a single overlooked defect can be enough to render the whole system insecure, unreliable, or inaccurate, and experience has proven that it is common for even the most capable experts to overlook flaws and defects in software. It is unreasonable to expect perfection from vendors or testing labs given the complexity of modern election technology. If the system is completely reliant upon software, failures and security flaws are inevitable.

The federal standards board recently endorsed a move towards software-independent systems. A software-independent voting system is one where undetected flaws in the software cannot cause undetectable errors in the election outcome. For instance, adopting voter-verified paper records and routine audits of those records would be one way to achieve software-independence, and it has the benefit of reducing our reliance upon the security of the software. In my opinion, software-independence would make the shortcomings of the certification process and the shortcomings of the technology less critical.

A second consequence is that the spread of electronic voting machines has degraded the transparency of our elections. Steps that once were performed by hand are now being done by computer, and votes are recorded and counted using secret, proprietary code. The secrecy surrounding the computer software makes it harder for the public to observe and exercise meaningful oversight over the administration of our elections. This loss of transparency was not intentional, but the effect is unmistakable nonetheless.

In this testimony, I outline several steps that could be taken to restore some of the transparency that has been lost in the transition to electronic voting. One of the most promising directions to improve transparency may be to conduct routine manual audits after every election and provide the public with opportunities to observe and oversee the process. This would enable robust oversight by the public at large. Ultimately, the success of our elections depends upon people, procedures, and public participation in the process.

Problems with today's systems

Federal standards call for voting machines to be tested by testing labs before the machines are certified for use. However, over the past few years we have learned that machines with reliability, security, and accuracy problems are receiving certification:

- *Lost votes.* Federally certified voting machines have lost thousands of votes. In Carteret County, NC, voting machines irretrievably lost 4,400 votes during the 2004 election. The votes were never recovered, and a re-vote in one very close statewide race was avoided only when one candidate conceded[1]. In 2002, vote-counting software in Broward County, Florida, initially mis-tallied thousands of votes, due to flaws in handling more than 32,000 votes; fortunately, alert election officials noticed the problem and were able to work around the flaws in the machines. In 2004, the same problem happened again in Broward County, changing the outcome on one state proposition[2] [3], and in Orange County[4]. In Fairfax County, Virginia, election officials were surprised to discover that a voting machine was erroneously subtracting a vote for one candidate for about one out of every hundred voters who used the machine[5]. In Tarrant County, Texas, a federally certified voting system counted 100,000 votes that were never cast by voters[6].

- *Reliability flaws.* Federally certified machines have suffered from reliability flaws that could have disrupted elections. California's reliability testing found that one federally certified

voting system suffered from mechanical and software reliability problems so severe that, if it had been used in a real election, about 20% of machines would have experienced at least one failure during election day and probably would have had to be taken out of service[7].

- *Security risks.* Federally certified machines have been found to contain numerous security defects that threaten the integrity of our elections. Over the past several years, we have been inundated with revelations of security flaws in our voting systems from academics (e.g., Johns Hopkins University, Rice University[8], University of California[9], Princeton[10], University of Connecticut[11], Florida State University[12]), industry consultants hired by election administrators (e.g., SAIC[13], Compuware[14], InfoSENTRY[15], and RABA[16]), and interested outsiders (e.g., Finnish researcher Harri Hursti[17] [18]). None of these flaws were caught by federal or state testing. In the past five years, at least eleven studies have evaluated the security of commercial voting systems, and every one found new, previously unknown security flaws in systems that had been approved by the testing labs. In my own research, I have found flaws in federally approved voting systems. Last year, I was commissioned by the State of California to examine the voting software from one major vendor, and I found multiple security flaws even though the software was previously approved at the federal and state level[19]. One of these flaws was discovered at least three times by independent security experts over a period of nine years (once in 1997, again in 2003, and again in 2006), but was never flagged by the testing labs at any point over that nine-year period[20]. This year, I participated as part of a team commissioned by the State of Florida to examine voting software from another major vendor, and I found multiple security flaws in that system as well even though the software was federally approved[21].

All of these defects were ostensibly prohibited by federal standards[22], but the testing and federal certification process failed to weed out these problematic voting systems. The consequence of these problems is that the federal certification process is at present unable to assure that voting systems meet minimum quality standards for security, reliability, and accuracy.

It is natural to ask what we can learn from past failures of the federal certification process. These failures have exposed structural problems in the federal certification process:

- *Conflict of interest.* The testing labs are paid by and chosen by the vendors whose systems they are evaluating. Testing labs are surely aware that withholding approval too frequently might send vendors to competing testing labs with a reputation for more lenient treatment. Elsewhere in the software industry, a similar "race to the bottom" has been observed in labs that test compliance to international computer security standards[23]. Thus, the testing labs are subject to conflicts of interest that raise questions about their ability to effectively safeguard the public interest. Unfortunately, at present there are few checks and balances that can be used to hold testing labs accountable if they fail to serve the public interest.

- *Insufficient transparency.* The process lacks transparency, rendering effective public oversight difficult or impossible and making it difficult to hold vendors or testing labs accountable. Under past practices, testing lab reports were proprietary—they were considered the property of the vendor—and not open to public inspection. Also, if a voting system fails testing, that fact was revealed only to the manufacturer of that voting system. In one widely publicized incident, one Secretary of State asked a testing lab whether it had approved a particular voting system submitted to the testing lab. The testing lab refused to comply: it declined to discuss its tests with anyone other than the voting system manufacturer, citing its policy of confidentiality[24].

In addition, the secretive nature of the elections industry prevents independent security experts from performing their own analysis of the system. Technical information about voting systems is often considered proprietary and secret by vendors, and voting system source code is generally not available to independent experts. In the rare cases where independent experts have been able to gain access to source code, they have discovered reliability and security problems.

- *Lax testing.* Testing is too lax to ensure that the machines are secure, reliable, and trustworthy. The federal standards require only superficial testing for security and reliability. For instance, California's tests have revealed unexpected reliability problems in several voting systems previously approved by testing labs. In my opinion, California's reliability testing methodology is superior to that mandated in the federal standards, because California tests voting equipment on a large scale and under conditions designed to simulate a real election.

- *Requirements not enforced.* Many standards in the requirements are not tested and not enforced. The federal standards specify many requirements that voting systems must meet, and specify a testing methodology for testing labs to use, but many of the requirements are not covered by that testing methodology. The testing labs only apply whatever tests are mandated by the standards. The consequence is that the federal standards contain many requirements with no teeth. For instance, Section 6.4.2 of the 2002 standards requires voting systems to "deploy protection against the many forms of threats to which they may be exposed"; the security vulnerabilities listed above appear to violate this untested requirement. Likewise, Section 6.2 requires access controls to prevent "modification of compiled or interpreted code"; four of the major vulnerabilities revealed in the past two years have violated this requirement—for instance, two systems were found to use weak passwords (one system "1111" used as the factory-set PIN). These requirements appear to be ignored during testing and thus have little or no force in practice.

- *The COTS loophole.* Parts of the voting software are exempt from inspection, reducing the effectiveness of federal testing. The federal standards contain a loophole that renders Commercial Off-the-Shelf (COTS) software exempt from some of the testing. The COTS loophole means that the security, reliability, and correctness of those software components are not adequately examined. COTS software can harbor serious defects, but these defects might not be discovered by the federal certification process as it currently stands.

- *Reporting loopholes.* Even if a testing lab finds a serious security flaw in a voting system, they are not required to report that flaw if the flaw does not violate the VVSG standards. Thus, it is possible to imagine a scenario where a testing lab finds a flaw that could endanger elections, but where the testing lab is unable to share its findings with anyone other than the vendor who built the flawed system. Relying upon vendors to disclose flaws in their own products is ineffective.

- *Disincentives to scrutiny.* There are disincentives for local election officials to apply further scrutiny to these machines. Some local election officials who have attempted to make up for the gaps in the federal certification process by performing their own independent security tests have faced substantial resistance. After one Florida county election official invited outside experts to test the security of his voting equipment and revealed that the tests had uncovered security defects in the equipment, each of the three voting system vendors certified in Florida responded by declining to do business with his county[25]. The impasse was resolved only

when the State of Florida interceded[26]. In Utah, one election official was pressured to resign after he invited independent security experts to examine the security of his equipment and the testing revealed security vulnerabilities[27] [28]. The disincentives to performing independent security testing at the local level heighten the impact of shortcomings in the federal standards. Fortunately, many public-minded election officials have placed the public interest first and insisted upon further scrutiny despite these disincentives.

- *No way to decertify.* Under the certification process in effect until recently, if serious flaws are discovered in a voting system after it has been approved, there is no mechanism to de-certify the flawed system and revoke its status as a federally qualified voting system.

The federal certification process is currently in flux. Responsibility for federal certification of voting systems has transferred from NASED, a non-governmental organization that previously conducted certification on a volunteer basis, to the Election Assistance Commission (EAC), a government agency which now has responsibility for the federal certification process. The testing labs are being re-examined and re-accredited by the EAC and the National Institute of Standards (NIST). The EAC has made several incremental changes to the federal certification process. These changes are going into effect for the first time this year, so it is too early to know what effect they may have.

The federal standards are also in flux. In 2005, the EAC adopted the 2005 Voluntary Voting System Guidelines (VVSG), a set of federal standards for voting systems. The 2005 VVSG were drafted over a period of approximately three months and represent only an incremental change to the federal standards; consequently, they do not address many of the fundamental issues I describe. The 2005 VVSG did not take effect until January 1, 2007. The EAC is currently overseeing the drafting of a second revision of the federal standards, dubbed "VVSG II". The VVSG II are expected to institute more sweeping changes to the standards, and are not expected to take effect until January 1, 2010.

The effects of revisions to these standards is delayed by several factors. First, the new standards do not take effect until two years after they are published by the EAC. Second, systems that are already deployed when the new standards take effect are grandfathered. Third, systems that were certified before the new standard takes effect are grandfathered. Today, most states allow local election officials to purchase equipment that was certified to the old 2002 standards, even though the 2005 VVSG have already "taken effect." Fourth, to recoup their investment in expensive voting equipment, most jurisdictions are reluctant to replace existing systems until it is absolutely necessary. Consequently, the effect of revisions to the standards is likely to be delayed significantly. We may need to wait until the middle of the next decade before most of our voting systems are certified to the VVSG II standards.

The EAC has made progress on a number of the structural problems in the federal certification process, but some issues remain:

- *Conflict of interest.* The testing labs continue to be paid by and selected by the vendors, under the EAC's certification process. The conflict of interest remains. At present the EAC lacks the statutory authority that would be needed to eliminate the conflict of interest.

- *Transparency.* The EAC has made significant improvements to the transparency of its certification process. Test reports and related documents will be made public, which is a significant step forward. However, the effect of this change will be delayed by many years. Only new voting systems submitted to the new EAC certification process benefit from this improvement to

transparency. Existing systems—including all currently deployed voting systems—are grandfathered, and their test reports remain proprietary. Because new voting technology is expected to diffuse into the market slowly in the future, I predict that most voters will continue to vote on systems that were tested in secret for many years.

Technical information and voting system source code remains proprietary and unavailable for inspection or analysis by independent experts, under the EAC certification process.

- *Lax testing.* The 2005 VVSG do not remedy the demonstrated failures of the process to screen out insecure, unreliable, and inaccurate machines. Testing for security and reliability remains inadequate under the 2005 VVSG.

  The VVSG II are expected to adopt a more rigorous test regimen similar to California's reliability testing. This shift seems likely to significantly improve the quality of reliability testing in the future. The VVSG II are also expected to contain provisions for more rigorous security testing, but the effectiveness of these provisions will be highly dependent upon how they are implemented. The effect of these changes will be delayed by many years, because of the delays before the VVSG II take effect and before vendors submit new systems for certification under the VVSG II.

- *Enforcement of requirements.* It is too early to tell whether the EAC certification process will do a better job of enforcing the requirements in the standards.

- *COTS.* The 2005 VVSG do nothing about the COTS loophole.

  The VVSG II make significant progress on this issue. The VVSG II are expected to narrow the exemption for COTS software, and to take other steps that will address many of the concerns regarding COTS software. I am optimistic that the VVSG II will mitigate the COTS issue. However, the effect of these improvements will be delayed by many years.

- *Reporting.* In its new certification process, the EAC has eliminated the loophole regarding reporting of systems that fail the testing process. When a voting system fails the tests, this fact will be reported publicly.

- *Disincentives.* The disincentives for local election officials to scrutinize voting systems more closely are not a product of the federal standards process and cannot be eliminated at the federal level. However, the EAC is free of many of these pressures and thus is in a unique position to take a leadership role in more closely scrutinizing the reliability, security, and trustworthiness of voting technology. That has not happened so far.

- *Decertification.* The EAC has made progress on this problem. The EAC has created a process for decertifying systems that were certified under the EAC's certification process, if serious flaws are discovered in those systems. However, there is still no mechanism for decertifying systems that were certified under the prior NASED certification process. All currently deployed voting systems fall under the latter category, and thus apparently cannot be decertified by any federal process.

In the short term, these shortcomings have several consequences:

- We are likely to continue to see new security and reliability problems discovered periodically. The security and reliability of federally approved systems will continue to be subject to criticism.

- Shortcomings at the federal level place a heavy burden on states. The 2005 standards do not provide enough information about the reliability and security of these machines to help states and counties make informed purchasing decisions. This places an undue burden on local election officials. Some states are doing their best to make up for gaps in the federal process, but many states do not have the resources to do so.

  Also, the increased scrutiny at the state level has the potential to subject vendors to dozens of involved state-level certification processes that have been instituted to make up for the gaps in the federal process, increasing the compliance burden on vendors and increasing equipment costs.

- For the next decade or so, millions of voters will continue to vote on voting machines that cannot be independently audited. This may diminish confidence in election results. In the event of any dispute over the outcome of the election, it may be impossible to demonstrate whether the election was accurate. Allegations of fraud may be difficult or impossible to rebut, due to the fact that today's paperless voting machines do not generate and retain the evidence that would be required to perform an effective audit. The lack of openness and transparency regarding voting system source code, testing, and equipment may spawn further distrust in voting systems.

- Voting equipment may still be subject to security and reliability problems, even if they comply with the 2005 standards. Many of the security and reliability defects described above would not have been prevented even if the 2005 standards had been in force when the machines were evaluated. Approval under the 2005 standards is not a guarantee of security or reliability.

In the long term, I am more optimistic. I expect the VVSG II to significantly improve the reliability, security, and trustworthiness of voting technology. These improvements may be delayed over a period of a decade or so, but I believe they will gradually but surely make a significant difference.

Potential ways to address certification-related shortcomings

There are several possible policy options that could be considered to address issues in the federal certification process:

- *Reduce dependence upon software.* One possibility is to reduce our dependence upon the certification process to vet voting software, by reducing our dependence upon software in elections.

  At present, the best tool we have for ensuring that votes are counted accurately is to use voter-verified paper records and perform routine manual audits of the paper records[29] [30]. Adoption of voter-verified paper records and routine audits would reduce our reliance on testing labs to ferret out security and reliability problems in the software.

  Paperless voting machines are problematic, because they demand an unachievable degree of perfection from voting machine vendors and federal testing labs. A single bug or defect in these machines can potentially cause undetectable errors in the election outcome and can potentially change the result of the election, perhaps without anyone realizing it. Given the complexity of modern voting systems, it is not reasonable to expect testing labs to eliminate the possibility of bugs or defects in voting software. This introduces the possibility that certified voting machines could be subject to failures or fraud that affect the election outcome. This risk

is exacerbated by the fact that paperless voting machines are not auditable. There is no effective way to independently check whether their results are accurate or to detect electronic fraud. The inability to audit these machines greatly heightens the impact of security-related defects. Ensuring that election results can be independently audited would go a long way to reducing our reliance upon testing labs to verify that voting software is free of material bugs or defects.

The TGDC, a body which helps to set federal voting system standards, has recently endorsed a requirement that voting systems be *software-independent*[31]. A voting system is considered software-independent if an undetected change or error in the voting software cannot cause undetectable changes or errors in the outcome of the election[32]. For instance, voting systems with a voter-verified paper record are considered software-independent, because the voter-verified paper records can be used to audit or recount the election results. Software-independence reduces the urgency of the shortcomings in the federal certification process, by reducing (but not eliminating) the impact that defects in the source code can have. In the long run, I expect this to have beneficial for election integrity.

In general, we can rate voting systems by the degree to which they rely on software:

- Paperless e-voting systems are completely dependent on the correctness of their software.
- Adding a VVPAT printer reduces the dependence on software.
- Paper-based optical scan systems reduce this dependence even further, and hand-counted paper ballots eliminate dependence on software.

Generally, the more the system depends on the correctness of its software, the greater the likelihood of reliability and security problems. Of course, software independence is just one among several considerations in the choice of a voting system.

Jurisdictions that use voter-verified paper records and routine manual audits are less dependent upon the federal certification process to identify problems. Adoption of paper ballots (whether optically scanned or manually counted) would further reduce the degree of dependence upon voting software and further reduce our reliance upon the federal certification process. While I expect the VVSG II to gradually drive a migration to software-independent voting systems over the next decade or so, the sooner that jurisdictions adopt software-independent systems, the sooner they will receive the associated benefits.

Currently, only 13 states have mandated use of these measures. (At present, 27 states mandate voter-verified paper records, another 8 states use voter-verified paper records throughout the state even though it is not required by law, and the remaining 15 states do not consistently use voter-verified paper records. Of the 35 states that do use voter-verified paper records statewide, only 13 require routine manual audits of those records[33].) Voter-verified paper records provide an independent way of reconstructing the voter's intent, even if the voting software is faulty or corrupt, making them a powerful tool for reliability and security. This provides a fallback in case of problems with the software or the electronic record of votes cast.

- *Improve local procedures.* The most effective and practical step that local election officials could take to make existing voting systems as secure and reliable as possible for upcoming elections would be to adopt the recommendations of the Brennan Center report on e-voting. These recommendations include:
  - Conduct automatic routine audits of the voter-verified paper records;

- Perform parallel testing of voting machines;
- Ban voting machines with wireless capability;
- Use a transparent and random selection process for all audits; and,
- Adopt procedures for investigating and responding to evidence of fraud or error.

Further information may be found in the Brennan Center report[34].

- *Eliminate conflicts of interest.* Congress could enable the EAC to eliminate conflicts of interest in the federal testing process. Testing labs should not be paid by the vendors whose systems they are testing. One possible solution would be for the EAC to collect a fee from vendors, when a voting system is submitted for certification, to cover the costs of hiring testing labs to evaluate the system under consideration. This would make the testing labs more directly accountable to the EAC. At present, EAC does not have statutory authority to collect a fee from vendors[35]. If Congress were to grant EAC this authority, the EAC could address the conflict of interest.

  Vendors should not choose which testing lab will evaluate their systems. Instead, the EAC should choose the testing lab. For instance, the EAC could assign each voting system to a testing lab selected at random from the list of accredited labs.

- *Consider mandating source code disclosure.* Broader disclosure of voting system source code would help to hold testing labs accountable and allow political parties, local election officials, and interested members of the public to "get a second opinion." The secrecy surrounding voting source code is a barrier to independent evaluation of machines and contributes to distrust. Disclosing voting source code more broadly could enhance transparency, improve public oversight, and help hold vendors and testing labs accountable. As a first step, source code could be made available to election officials or to independent technical experts under appropriate nondisclosure agreements. In the long run, source code could be publicly disclosed.

  Source code disclosure does not prevent vendors from protecting their intellectual property; vendors can continue to rely on copyright and patent law for this purpose.

  Keeping source code secret is not an effective security strategy: in the long run, the software cannot be kept secret from motivated attackers with access to a single voting machine. However, disclosing source code more broadly could enhance public confidence in elections and is could lead to improvements to voting system security.

  Source code disclosure is a complex issue. Because of space considerations, I have omitted many details and nuances. For more discussion of the policy issues surrounding source code disclosure, I refer the interested reader to my testimony on this subject before the Elections Subcommittee of the House Administration Committee[36].

- *Learn from field experience.* It would help to incorporate closed feedback loops into the regulatory process. Standards should be informed by experience. At present, there is no requirement for reporting of performance data or failures of voting equipment, no provision for analyzing this data, and no process for revising regulations in a timely fashion in response. It would help if there were a framework for collecting, investigating, and acting on data from the field and should provide a mechanism for interim updates to the standards to reflect newly discovered threats to voting systems. For instance, the FAA requires airplane operators to report all incidents (including both failures and near-failures), uses independent accident investigators to evaluate these reports, and constantly revises regulations in response to this

information. Adopting a similar framework for voting systems would likely improve voting systems.

At present, the regulatory process does not provide any mechanism for investigating failures or problems with equipment in the field. When an airplane crashes, federal crash investigators descend upon the scene to learn what went wrong so we can learn from our failures and ensure that it won't happen again. The election community does not have any mechanism for performing this kind of investigatory function.

Transparency

Historically, one of the abiding principles of election administration has been that the best way to demonstrate that the election is honest is by inviting public scrutiny and being open and transparent about all aspects of the election. When any aspect of election administration is kept secret, it invites questions about whether the secrecy is intended to cover up problems or to stifle debate.

The trend in elections is towards automation of more and more tasks that were previously performed manually. However, the spread of automation has unintentionally come with the unfortunate side-effect of degrading transparency[37] [38] [39]. When poll workers run elections or election officials count ballots, the public can observe that these actions are being performed correctly and openly, and can spot any errors or problems. In contrast, when those same operations are performed by machines containing proprietary technology, the secrecy surrounding those machines and their programming may prevent the public from meaningfully observing or engaging in oversight of the process.

There are several steps that could be taken to restore some of the transparency that has been lost:

- *Routine manual audits.* The single most important step that local election officials could take to improve transparency would be to institute routine manual audits and allow public observation of these audits. These audits should include a transparent and random process for selecting a random sample of precincts or machines, followed by a manual hand-to-eye recount of those voter-verified paper records.

  Audits provide a way to assess the accuracy of voting software. They are one of the few opportunities for a voter to verify that the votes were counted and tabulated correctly by the voting equipment. Election officials should ensure that interested parties are able to observe all aspects of the audit and see for themselves that the votes were counted accurately. Officials should also use audits to measure how accurate their equipment and processes are, to identify shortcomings, and to improve their processes for future elections. Officials should perform an audit after every election and publish the results of the audit and the cause of every discrepancy or error detected during the audit.

- *Broader disclosure of technical information.* There has recently been considerable public debate about the trustworthiness of voting machines. Some have argued that current voting machines are severely flawed; others have disputed that characterization. However, because of the secrecy surrounding proprietary voting software, advocates on both sides of the debate have often been denied access to the information that would be needed to present evidence for their position. The result is that advocates are all too often forced to argue from first principles or based on their professional judgement, rather than from hard evidence.

  Reversing the presumption of secrecy for technical information about voting technology would make it possible to have a more informed debate on the trustworthiness of today's e-voting

machines. In particular, disclosure of source code would allow interested parties to analyze the software for themselves, without having to rely upon analysis from some testing lab. We could expect and insist that anyone who wants to argue that the voting software from one vendor is flawed should be able to point to where exactly in the source code the flaw may be found. We could expect and insist that anyone who wants to argue that the voting software is flawless should be able to show evidence that the source code is free of flaws. This would create the opportunity for a more informed and scientific debate regarding the trustworthiness of e-voting, and it might raise the level of the debate.

Activities of the ACCURATE center

As I have studied electronic voting, I have become convinced of the importance of research into better voting technology. In 2005, I was fortunate to be part of a team that received funding from the National Science Foundation (NSF) to form a center called A Center for Correct Usable Reliable Auditable and Transparent Elections (ACCURATE). The ACCURATE grant provides a total of $7.5 million in funding over five years. The mission of the ACCURATE center is to study electronic voting. We are exploring the design space for voting machines so we can better understand how the next generation of these machines should be constructed. ACCURATE researchers include a psychology professor, a law professor, and eight computer scientists.

The three primary goals of ACCURATE are research, outreach, and teaching. Our research focuses on developing technologies that can improve voting systems. Our outreach effort focuses on working with the elections community to help them understand technology and policy issues. For example, we participated in post-election audits in 2006. Finally, we have designed curriculum to teach our students about the important issues in electronic voting.

Our ACCURATE research consists of several thrusts. One ACCURATE project involves performing usability testing to compare different types of equipment. ACCURATE researchers test design prototypes against human subjects to find out whether they are usable. We also provide coordinated responses to requests, such as those from the EAC. For example, we provided detailed comments on the proposed voting standards. In addition, we are performing basic research in computer security to create technology for future generations of voting systems. More information about the activities of ACCURATE may be found in our 2006 annual report[40].

Notes

[1] "Computer loses more than 4,000 early votes in Carteret County", Associated Press, Nov. 4, 2004.

[2] "Broward Ballot Blunder Changes Amendment Result", Local 10 News, Nov. 4, 2004.

[3] "Broward Machines Count Backward", The Palm Beach Post, Nov. 5, 2004.

[4] "Distrust fuels doubts on votes: Orange's Web site posted wrong totals", Orlando Sentinel, Nov. 12, 2004.

[5] D. Cho, "Fairfax Judge Orders Logs Of Voting Machines Inspected", Washington Post, p.B01, Nov. 6, 2003. `http://www.washingtonpost.com/ac2/wp-dyn/A6291-2003Nov5`

[6] "Vote spike blamed on program snafu", Forth Worth Star-Telegram, Mar. 9, 2006.

[7] M. Bishop, L. Guarino, D. Jefferson, D. Wagner, "Analysis of Volume Testing of the AccuVote TSx/AccuView", Report of the California Secretary of State's Voting Systems Technology Assessment Advisory Board, Oct. 11, 2005.

[8] T. Kohno, A. Stubblefield, A.D. Rubin, D.S. Wallach, "Analysis of an Electronic Voting System", May, 2004.

[9] D. Wagner, D. Jefferson, M. Bishop, C. Karlof, N. Sastry, "Security Analysis of the Diebold AccuBasic Interpreter", Report of the California Secretary of State's Voting Systems Technology Assessment Advisory Board (VSTAAB), Feb. 14, 2006.

[10] A.J. Feldman, J.A. Halderman, E.W. Felten, "Security Analysis of the Diebold AccuVote-TS Voting Machine", Sept. 2006.

[11] A. Kiayias, L. Michel, A. Russell, A.A. Shvartsman, "Security Assessment of the Diebold Optical Scan Voting Terminal", Oct. 30, 2006.

[12] A. Yasinsac, D. Wagner, M. Bishop, T. Baker, B. de Medeiros, G. Tyson, M. Shamos, and M. Burmester, "Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware", Feb. 23, 2007.

[13] "Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes", Science Applications International Corporation, Sept. 2, 2003.

[14] "Direct Recording Electronic (DRE) Technical Security Assessment Report", Compuware Corporation, Nov. 21, 2003.

[15] "Security Assessment: Summary of Findings and Recommendations", InfoSENTRY, Nov. 21, 2003.

[16] "Trusted Agent Report: Diebold AccuVote-TS System", RABA Innovative Solution Cell, Jan. 20, 2004.

[17] H. Hursti, "Critical Security Issues with Diebold Optical Scan", Black Box Voting, July 4, 2005.

[18] H. Hursti, "Critical Security Issues with Diebold TSx", Black Box Voting, May 11, 2006.

[19] D. Wagner, D. Jefferson, M. Bishop, C. Karlof, N. Sastry, "Security Analysis of the Diebold AccuBasic Interpreter", Report of the California Secretary of State's Voting Systems Technology Assessment Advisory Board (VSTAAB), Feb. 14, 2006.

[20] D.W. Jones, "Connecting Work on Threat Analysis to the Real World", June 8, 2006.

[21] A. Yasinsac, D. Wagner, M. Bishop, T. Baker, B. de Medeiros, G. Tyson, M. Shamos, and M. Burmester, "Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware", Feb. 23, 2007.

[22] For instance, the security vulnerabilities appear to violate the requirements of Section 6.4.2 and Section 6.2 of the 2002 FEC standards.

[23] R.J. Anderson, *Security Engineering – A Guide to Building Dependable Distributed Systems*, Wiley, 2001, §23.3.

[24] "Election Officials Rely on Private Firms", San Jose Mercury News, May 30, 2004.

[25] "Election Whistle-Blower Stymied by Vendors", Washington Post, Mar. 26, 2006.

[26] "Sort of fixed: Broader election flaws persist", Tallahassee Democrat, Apr. 15, 2006.

[27] "Cold Shoulder for E-voting Whistleblowers", The New Standard, May 17, 2006.

[28] "New Fears of Security Risks in Electronic Voting Systems", The New York Times, May 12, 2006.

[29] D.W. Jones, "Auditing Elections", Communications of the ACM 47(10), Oct. 2004, pp.46-50.

[30] A.D. Rubin, Written testimony before the Election Assistance Commission, June 30, 2005. `http://avirubin.com/vote/eac2.pdf`

[31] TGDC Resolution #06-06, "Software Independence of Voting Systems," Dec. 5, 2006.

[32] R.L. Rivest, J.P. Wack, "On the notion of 'software independence' in voting systems", `http://vote.nist.gov/SI-in-voting.pdf`.

[33] "The Machinery of Democracy: Protecting Elections in an Electronic World", Brennan Center Task Force on Voting System Security, June 27, 2006. Since that report was written, Arizona has adopted voter-verified paper records and routine manual audits of those records statewide.

[34] "The Machinery of Democracy: Protecting Elections in an Electronic World", Brennan Center Task Force on Voting System Security, June 27, 2006.

[35] United States Election Assistance Commission, "EAC's Testing and Certification Program for Voting Systems", Jan. 19, 2007.

[36] D. Wagner, Written testimony before the Elections Subcommittee of the House Administration Committee of the U.S. House of Representatives, Mar. 15, 2007. `http://www.cs.berkeley.edu/~daw/papers/testimony-house07.pdf`

[37] D.W. Jones, "Voting System Transparency and Security: The need for standard models", written testimony before the EAC Technical Guidelines Development Committee, Sept. 20, 2004. `http://www.cs.uiowa.edu/~jones/voting/nist2004.shtml`

[38] J. Hall, "Transparency and Access to Source Code in E-Voting," USENIX/ACCURATE Electronic Voting Technology (EVT'06) Workshop. `http://josephhall.org/papers/jhall_evt06.pdf`

[39] D.K. Mulligan, J.L. Hall, written testimony before the California Senate Elections, Reapportionment & Constitutional Amendments Committee, Feb. 8, 2006. `http://josephhall.org/nqb2/media/Mulligan_Hall_OSHRG_Statement.pdf`

[40] ACCURATE, 2006 Annual Report, Feb. 2, 2007. `http://accurate-voting.org/2007/02/02/annual-report/`