Statement of

Eric A. Fischer
Senior Specialist, Science and Technology
Resources, Science, and Industry Division
Congressional Research Service
Library of Congress

Before the
Security and Transparency Subcommittee
Technical Guidelines Development Committee
Election Assistance Commission

Public Hearing

September 20, 2004

Thank you, Mr. Chairman and members of the subcommittee, for inviting me to speak with you today at this hearing on computer security and transparency in voting systems. I understand that you are examining voting system security and transparency in a comparative and historical context, and the lessons and principles that can be derived from this larger context, as it applies to the mission of the Technical Guidelines Development Committee, to develop recommendations for the Election Assistance Commission with respect to voluntary voting system guidelines.

I serve as Senior Specialist in Science and Technology at the Congressional Research Service. CRS is the public policy research arm of the United States Congress. We are a legislative branch agency within the Library of Congress. We perform nonpartisan, objective analysis and research on legislative issues for Members of Congress, their committees and staff. In keeping with that mission, we do not take positions, make recommendations, or advocate on policy issues, and I will not do so today.

My involvement with election reform began in November 2000, when we anticipated that the 107th Congress might be interested in examining strengths and weaknesses of different kinds of voting systems. Subsequently, my colleagues and I provided extensive support to Congress in deliberations that led to the enactment of the Help America Vote Act of 2002 (HAVA). We continue to provide support to Congress with respect to HAVA implementation and oversight.

Most of the recent public debate about voting systems has focused on electronic voting systems (DREs).[1] However, more than two-thirds of the American electorate will use other voting systems in the coming election. Roughly a third will vote with optical scan ballots, and another third with punchcard or lever machines.[2] As the November 2000 and many other elections have demonstrated, significant issues may arise with respect to any voting system, especially in close elections. With respect to security and transparency of voting systems, there are several points in particular that I think the subcommittee might find useful to keep in mind:

1. A wide diversity of voting systems are used in the United States — optical scan, direct recording electronic (DRE), punchcard, lever machine, and hand-counted paper ballot systems. There are also several different models for each kind of system. Each system and model has different characteristics and different security vulnerabilities. To the best of our knowledge, there has been no comparative risk assessment done with respect to security for the different systems. Most of the focus has been on DREs, for which some assessments have been performed and have received national attention.

---

[1] See also Eric A. Fischer, *Voting Technologies in the United States: Overview and Issues for Congress*, CRS Report RL30773, 21 March 2001; ————, *Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues*, CRS Report RL32139, 4 November 2003; and ————, *Electronic Voting Systems (DREs): Legislation in the 108th Congress*, CRS Report RL32526.

[2] Election Data Services, "New Study Shows 50 Million Voters Will Use Electronic Voting Systems, 32 Million Still with Punch Cards in 2004," Press Release, 12 February 2004.

2. Voting systems are expected to meet several goals, some of which are potentially competing or conflicting with each other. They are expected to be highly affordable, very reliable, accurate, voter-friendly, secure, and accessible, and they are expected to produce results very quickly.
3. Elections are a connected set of complex systems and it is useful to view security issues in that context. This means that factors that are not themselves related to security may have significant consequences for security. It also means that changes made in one part of the complex may have unintended and even unpredictable effects on other parts.
4. The evolution of voting system security can be viewed in part as a kind of arms race, with each security innovation being answered with attempts to defeat it. This means that a completely secure voting system, while a laudable goal, is not likely to be achievable. It also means that attempts to defeat security should be expected.
5. Taken together, the previous two points strongly suggest that security solutions focusing primarily on technology are likely to fail. It is widely accepted that the best security solutions use a layered defense that involves personnel and procedural controls as well as technology and that is applied throughout the entire system or process. The TGDC may wish to consider such a life-cycle approach with respect to the development of its recommended guidelines.
6. The voting system requirements in the Help America Vote Act (HAVA) do not explicitly address security, except for requiring an audit capacity for the voting system. In light especially of the recent controversy about voting-system security, this may place a particular burden on the TGDC to address security issues in the guidelines.
7. Just as no voting system is completely secure, no voting system is completely transparent either. With current technology, the need for a secret ballot prevents the voter from knowing whether his or her vote was counted accurately, no matter what voting technology is used. However, some technologies in development may dramatically improve transparency, and the TGDC might wish to consider such possibilities as it develops its recommended guidelines.
8. The current federal voting systems standards address only computer-assisted voting. About 80% of voters are expected to use computer-based systems this November — whether optical scan, punchcard, or DREs. No federal guidelines currently exist for the systems used by the other 20% of voters — namely, lever machines and hand-counted paper ballots. While the use of such systems is likely to continue declining, they are unlikely to disappear soon, and guidelines for them might be appropriate.

I would like to use my remaining time to elaborate on a few of the above points.

Voting System Security. Many innovations that have become familiar features of modern elections originated at least in part as a way to reduce election fraud such as tampering with ballots to change the vote count for a candidate or party. However, as each such innovation was introduced, miscreants began looking for ways to defeat its security features. This is why the evolution of voting systems can be viewed in part as a

kind of arms race, with each subsequent security innovation being answered with attempts to defeat it.

For example, after a series of scandals involving vote-buying in the 1880s, calls for reform led to widespread adoption of the Australian secret ballot. While providing improved security over the previous ticket-ballot system, the Australian secret ballot did not eliminate tampering. Ballots could still be removed, spoiled, or altered by corrupt pollworkers, or even substituted or stuffed, although with greater difficulty than with ticket ballots. The Australian ballot also did not eliminate the possibility of vote-buying or coercion, but it arguably made them more difficult. However, the forms of tampering evolved in response to this technological innovation, with miscreants finding new ways to add, subtract, or alter ballots. But evidence of vote fraud, even to the present day, tends to be anecdotal because of inherent problems in detecting and prosecuting such fraud. It is difficult to identify either the most prevalent type of vote fraud or where it is most likely to occur. Our decentralized system of running elections may help prevent large-scale vote fraud, but it also makes gathering information on fraud or attempts at fraud a difficult task.

One way to eliminate some means of ballot tampering is to eliminate document ballots. That became possible with the introduction of the lever voting machine in 1892. The lever machine eliminates the need to count ballots manually. Instead, pollworkers read the numbers recorded by counters inside the machine. Because there is no document ballot, recounts and audits are limited to review of totals recorded by each machine. Of course, tampering is also possible with lever machines. For example, the mechanisms could be adjusted so that the counter does not always advance when a particular candidate is chosen.

Computer-assisted vote counting was first introduced in the 1960s, with punchcard systems. Direct recording electronic systems (DREs) were first used in the 1970s. Like lever machines, they do not use document ballots. Optical scan systems debuted in the 1980s. Like lever machines, machine counting made some kinds of tampering more difficult, but it did not eliminate them, and it created new possibilities for tampering with the counting software and hardware.

Security requirements and measures vary among the technologies used. Document ballots require security measures and controls from the initial printing of the ballots through counting and storing them. However, the ballots can serve as a basis for an audit trail. Such an audit trail of individual ballots is not available for lever machines or DREs.[3] Experts differ on the importance of such a paper audit trail for ensuring the security and integrity of the voting process. Special measures and controls have also been developed for both hardware and software used in computer-based systems, and other kinds of audit trails are possible, for example, records of individual events that occurred during the course of use.

[3] DREs record individual ballot records, but these are not truly independent — they are essentially the same votes recorded in the counting registers but in a different format.

Pre- and postelection tests are widely performed on voting-machine systems to check for accuracy and also to guard against tampering. In addition, manual recounts may be routinely performed on a small percentage of ballots as a check on the validity of the machine count. However, such sample recounts may not be very effective at detecting counting problems.[4] Accurate operational tests are most difficult with DRE and lever-machine systems, where there is no ballot document and the count is recorded separately at each voting booth. A thorough test would require hundreds of simulated votes to be placed on each machine.

Ballot secrecy is widely considered a crucial mechanism for preventing vote tampering and fraud. Two basic aspects of ballot secrecy are first, that once a ballot is cast, it cannot be traced by a second party to an individual voter, and second, that a voter cannot demonstrate to others how he or she voted. Modern polling-place voting ensures that voters cast secret ballots in two ways. First, voter identification and ballot casting are performed in two separate steps. Second, ballots are filled out and cast in such a way that no one else can observe what choices the voter made, except where assistance is requested.

The impact of vote tampering depends on several factors. Two of the most important are the scale of an attack and the competitiveness of the contest. An attack would have to have sufficient impact to affect the outcome of the election. For that to happen, scale is critical. If tampering impacts only one ballot or one voting machine, the chances of that affecting the election outcome would be small. But tampering that affects many machines or the results from several precincts could have a substantial impact, although it might also be more likely to be detected. The scale of attack needed to affect the outcome of an election depends on what proportion of voters favor each candidate. The more closely contested an election is, the smaller the degree of tampering that would be necessary to affect the outcome. Similarly, it would usually be easier to affect the election result for a local office than a statewide office because fewer votes would need to be added or subtracted from the total.

While attacks that added, subtracted, or changed individual votes are of particular concern, other kinds of attacks also need to be considered. One type of attack might gather information that a candidate could use to increase the chance of winning. For example, if vote totals from particular precincts could secretly be made known to operatives for one candidate before the polls closed, the results could be used to adjust get-out-the-vote efforts, giving that candidate an unfair advantage. Another type of attack might be to disrupt voting. The resulting delays could reduce turnout, perhaps to the benefit of one candidate, or could even cause voters to lose confidence in the integrity of the election in general. The latter might be of more interest to terrorists or others with an interest in having a negative impact on the political system generally. However,

[4] For example, if errors occurred at five out of 100 precincts, a simple mathematical analysis predicts that recounting 1% would have a 5% chance of detecting the problem — that is, 95 out of 100 times no problem would be detected. A 5% recount would yield only a 30% chance of detection. It would be necessary to recount 8% to achieve a 50% chance of discovering one of the problem precincts. To achieve a 95% chance of detecting one problem precinct would require recounting 20%.

disruptions and delays resulting from other sources, such as procedural errors, machine malfunctions, or even power outages, are well documented and can also have negative effects on public confidence.

In fact, security and reliability are related. Each election cycle, most voting systems work properly and without incident, but every cycle also brings reports of problems — whether they be malfunctioning machines or procedural errors. These are generally, and no doubt appropriately in most cases, treated as unintentional mishaps rather than deliberate attempts at tampering. However, the more common such problems are, the easier it may be for a miscreant to mask an attempt at tampering as a malfunction, just as, if a home computer tends to crash a lot, a crash caused by a virus might be treated as normal behavior. Consequently, improvements in reliability may contribute significantly to security.

Those kinds of attacks are potential threats against any voting system. However, the growing use of information technology in elections has had unique impacts on the threat environment. It provides the opportunity for new kinds of attacks, from new kinds of attackers. As information technology has advanced and cyberspace has grown, so too have the rate and sophistication of cyberattacks in general. There is no reason to believe that information technology used in the electoral process would be spared this trend.

Vulnerabilities. Like any complex system, voting systems exhibit vulnerabilities that attackers may seek to exploit. It can be useful to think of these in two categories — technical and social. Technical vulnerabilities may include such things as weaknesses in computer code, exposure of systems to tampering, and lack of auditing transparency. These potential weaknesses need to be considered not only for DREs but other systems as well. Optical scan and punchcard counters use computer code and are therefore potentially subject to several of the kinds of manipulation that has been so widely discussed for DREs. Similarly, punchcard and optical scan readers that are connected to the Internet, either directly or indirectly, are potentially exposed to electronic attack. Auditing transparency is an issue for lever machines because the voter cannot know if the machine recorded the choices the voter made or some other choices, and an observer also cannot check to see if all votes cast are counted correctly. The latter problem also exists with an optical scan or punchcard ballot reader, but there is a document ballot that can be checked independently.

Social vulnerabilities can include weaknesses relating to policy, procedures, and personnel. A security policy lays out the overall goals and requirements for a system and how it is implemented, including the technology itself, procedures, and personnel. An absent or weak policy, or even a good one that is not implemented properly, is considered a substantial vulnerability. Security policies of election administrators, vendors, third-party suppliers, and the testing authorities (ITAs) are all relevant, especially for computer-assisted voting. The security policy provides the basis from which procedures such as access controls are developed. Election administration is a complex effort involving vendors, ITAs, state and local government, and pollworkers who are often

volunteers, as well as voters. As with any security policy, inadequate or poorly implemented procedures can create serious vulnerabilities.

Perhaps the most important single factor in determining the vulnerability of a system is the people involved. It is they who must implement security policies and procedures and defend against any attacks. If they are not adequately skilled and trained, they may be unable to prevent, detect, and react to security breaches, and they may themselves be more vulnerable to a "social engineering" attack. In addition, it can be particularly difficult to defend against attack by an insider, so background checks and other controls to minimize that risk are especially important. This vulnerability may be compounded by two factors: pollworkers are largely a volunteer force, and local election officials rely on these volunteers by necessity to staff the polling places where votes are cast. Recruiting pollworkers is an ongoing, challenging responsibility.

While any voting system is potentially vulnerable to attack, it can be defended. It can be useful to think of three goals of defense from an attack on a computer-based system: protection, detection, and reaction. *Protection* involves making a target difficult or unattractive to attack. For example, good physical security can prevent attackers from accessing voting machines in a warehouse or at the polling place between the time machines are delivered and pollworkers arrive. Use of encryption and authentication technologies can help prevent attackers from viewing, altering, or substituting election data when it is transferred electronically.

Currently, election jurisdictions and vendors appear to rely heavily on procedural mechanisms for protection. These may include access controls, certification procedures, pre-election equipment-testing, and so forth. Such procedures are an essential element of an effective defense, but they must be implemented and followed properly if they are to ensure adequate protection. However, in some circumstances, the time and resources needed to follow such procedures may conflict with other important goals, such as the timely administration of an election, forcing election officials to choose whether to risk bypassing or modifying security procedures.

Detection involves identifying that an attack is being or was attempted. For example, election observers can serve as detectors of a potential attack. One approach is the use of auditing. Cryptographic protocols may also be useful in detecting attempts at tampering with computer-assisted systems.

Reaction involves responding to a detected attack in a timely and decisive manner so as to prevent its success or mitigate its effects. For example, if an observer sees something suspicious during voting or tallying, the process can be stopped and the situation investigated. Also, a tabulator may be programmed to shut down if certain kinds of problems are encountered. The system might also have additional defense measures such as antivirus software.

Unintended Consequences. Elections can be viewed as a connected set of complex systems. In general, imposing changes on complex systems may have unintended and

even unpredictable effects, especially where there is substantial variation among the individual systems and different sets. There are some nine thousand election jurisdictions in the United States — both counties and townships — and there are many differences in the ways they run elections. Election administrators often point out that every jurisdiction, and every election, is different. While it is not possible to completely eliminate the problem of unintended consequences, it can be addressed to some extent, for example by examining how well a practice has worked in a variety of election settings, just as software manufacturers test bug fixes under a variety of possible configurations before releasing them.

Failure to adequately consider such unintended consequences can have significant negative impact. A brief consideration of provisional balloting may provide an example. The core goal of provisional voting is to ensure that every valid voter has an opportunity to cast a ballot — that no registered voter is erroneously disenfranchised at the polling place. One approach might be simply to make sure that every voter who is not listed as registered is offered a provisional ballot, as HAVA requires. Such an approach would be simple and easy to administer, and it would ensure that no voter was turned away from a polling place. Suppose, however, that a voter is actually registered in a different precinct, and that state law requires each voter to cast the ballot in the precinct where he or she is registered, or the ballot will not be counted. In that case, which applies in several states, an approach intended to ensure enfranchisement would actually have the opposite effect.

Security in depth. It is generally accepted that defense should involve a focus on three elements: personnel, technology, and operations. The personnel component focuses on a clear commitment to security by an organization's leadership, assignment of appropriate roles and responsibilities, implementation of physical and personnel security measures to control and monitor access, training that is appropriate for the level of access and responsibility, and accountability. The technology component focuses on the development, acquisition, and implementation of hardware and software. The operations component focuses on policies and procedures, including such processes as certification, access controls, management, and assessments. A focus that is not properly balanced among those elements creates vulnerabilities.

An effective defense cannot be focused only on one particular location but needs to operate at all relevant points in the entire enterprise. For voting systems, these points would likely include development (both hardware and software) by the manufacturer, the certification process, acquisition of the voting system (including software and hardware updates) by the state, state and local implementation, and use during elections.

Finally, an effective defense is based on the assumption that attackers will continuously attempt to breach the defenses (including devising new ways to attack) and that they will eventually find a vulnerability to exploit. Therefore, a successful defense should be robust, so that security needs are met even if an attack occurs. One way to accomplish this is through a layered defense, in which more than one defense mechanism is placed between the attacker and the target. If the outer layer is breached, the next comes into play. Each layer should include both protection and detection capability. For example, a

state will use a combination of physical security (e.g., lock and key), procedural controls (e.g., who is given access to the system and for what purpose) and auditing (a record of what was done and by whom) to defend against tampering with voting systems.

Transparency and observability of the electoral process. This longstanding election principle is based on the notion that balanced observation of the process by partisan representatives and neutral third parties is the best way to ensure that an election is fair and accurate. This principle has taken on added importance given voting problems in the last presidential election and changes required by HAVA since then. It requires that key points in the election process, from voter registration and ballot preparation through certification of the results, be open and transparent, while preserving critical features such as ballot secrecy. For example, it is widely accepted that ballot boxes should always be in joint possession of, or observable by, representatives of at least two competing political parties from the time the boxes are first inspected before polls open to when they are emptied after polls close.

The use of electronic or mechanical machinery to aid in elections creates special challenges with respect to this principle. Even though most of the recent attention on this issue has focused on electronic voting machines (DREs), optical scan and punchcard systems, and even lever machines, all have "black box" characteristics in that votes are counted in a way that precludes human observation. Nevertheless, transparency and observability can be applied to these systems by such steps as taking full advantage of auditing capabilities, and ensuring that all actions, such as service to a machine by a technician, are observed and that the observers have sufficient technical understanding to assess the legitimacy of the actions taken.

Verifiability is usually thought of as an important aspect of transparency. It can be thought of as consisting of two components. One involves the capability of the voter to verify that his or her ballot was cast as intended. This is what is usually meant by *voter verifiability*. The other involves the capability to determine that the final tally accurately reflects all votes as cast by the voters and that it includes no additional votes — in other words, that no votes were improperly changed, omitted, or added. This has been called *results verifiability*. If all voters can obtain both voter and results verifiability, that is known as *universal verifiability*. Roll-call voting provides robust universal verifiability — voters publicly record their votes, which are counted in the presence of all voters. However, this approach sacrifices ballot secrecy and can be used only for very small electorates. While ballot secrecy reduces the risk of vote selling and coercion, it complicates verifiability, since voters cannot know directly if their ballots were counted as cast. Hand-counted paper ballot systems, which can provide ballot secrecy, may provide universal verifiability only under some very limited circumstances and only for very small electorates. Such systems can provide a kind of surrogate results verifiability, if observers closely watch the counting of ballots, but even that can be difficult to achieve. Lever machines and computer-assisted voting systems arguably exhibit neither voter nor results verifiability, although document-based systems such as optical scan and punchcards do retain the capacity for surrogate results verifiability if manual recounts are done in the presence of observers.

Some observers believe that the potential security problems associated with the lack of transparency and observability in vote casting and counting with nondocument systems such as DREs cannot be resolved through the use of security procedures, standards, certification, and testing. They assert that the only reliable approach is to use ballots that voters can verify independently of the DRE and that these ballots become the official record for any recounts. Others assert that voter verifiability is a highly desirable feature but caution about some of the proposed ways of achieving it. Still others believe that there are problems with the approach that make it undesirable.

HAVA requires that each voting system produce a paper audit record for the system and that this be the official record for recounts. It also requires that voters have the opportunity to correct their ballots before that record is produced. However, it does not stipulate that that record consist of individual ballots or that it be verifiable by the voter.

I hope that the subcommittee has found the evidence I have presented today helpful. I would be happy to answer any questions you might have.