Statement of

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

Before the
Election Assistance Commission

Public Hearing

June 3, 2004

Congressional Research Service Washington, D.C. 20540-7450

Thank you, Mr. Chairman and commissioners, for inviting me to speak with you today at this hearing on best practices, problems and transition issues associated with optical scan, punchcard, and lever machine voting systems and provisional voting.

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). I would like to mention in particular Analyst in American National Government Kevin Coleman, with whom I have worked closely on these issues. We continue to provide support to Congress with respect to HAVA implementation and oversight.

Before turning to best practices, it may be helpful to discuss some problems and issues with the voting systems being examined in this hearing. In our research, we have identified in particular issues associated with ballot design and usability of voting systems, the role of voting technology in contributing to voter error, the accuracy of counts and recounts, and voting system security.[1]

Most of the recent public debate about voting systems has focused on electronic voting systems (DREs). 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.

Ballot design and Voter Error. Designing a ballot is not a simple art, and standards vary from state to state. It is useful to distinguish between document ballots and posted ballots. A document ballot is the sheet of paper or cardstock on which a voter's ballot choices are recorded with an optical scan, punchcard, or hand-count system. A posted ballot is the presentation of candidate choices with a lever machine, DRE, or Votomatic-type punchcard system. For example, with a lever machine, identifying information is posted next to the corresponding levers. With punchcards (except Datavote, where the contests are printed on the ballot card), a voting booklet affixed to the voting device

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

[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.

presents the ballot choices. Punchcards are the only system that uses both a document and posted ballot.

A well-designed ballot of either type provides a fair and clear presentation of choices to the voter while minimizing the risk of unintended choices by the voter as well as unintentional undervotes, overvotes, and ballot spoilage. Issues of fairness include factors such as the order of presentation of candidates and the use of uniform typefaces. Those are usually addressed by state law or regulation. For example, some states require alphabetical presentation of candidates, and some require that the order of presentation be rotated for different parties from one election to another or even among precincts during the same election.

Fulfilling different goals for ballot design often involves trade-offs. For example, election officials may wish to enhance the readability of a ballot by using a fairly large typeface. If, however, there is a long list of candidates for an office, that may require splitting the list between two separate pages of a punchcard ballot book, as was done for the Presidential contest in Duval County, Florida, in the November 2000 election, or placing them on facing pages — the so-called butterfly ballot used in Palm Beach County. Both designs are thought to have unintentionally contributed to errors by voters, although in different ways.

The length, complexity, and manner of presentation of the ballot (which depends in part on the voting technology used) may all have some effect on the prevalence of undervoting. It may even vary depending on whether the ballot items are all placed on one page or several pages, and the position of an item on the page.

Also, different voting technologies place different constraints on the way a ballot can be designed to improve its clarity and ease of use. For example, some research indicates that certain voters may tend to undervote on contests at the top of the ballot when voting on a lever machine. In contrast, voters may be more likely to miss contests toward the end of a multipage punchcard ballot.

Undervotes may occur not only if the voter misses a contest, but also if the ballot is not marked correctly. For example, a mark made on an optical scan ballot may be too faint or small to be detected by the tabulator, or a voter might have made the marks with a type of pencil or pen that the tabulator cannot read. With Votomatic-type punchcards, a chad on a ballot might not be removed completely — the so-called hanging chad. These may result from several factors, such as incorrect use of the punching stylus by a voter, misalignment of the card in the voting device (which may be caused by a voter or a faulty device), or a voting device filled with chads from previous uses. The problems that incompletely removed chads can create in elections is well known.

Voting technologies differ in the degree to which they help a voter prevent or correct errors, and consequently, the incidence of voter error varies to some extent with the technology employed. Lever machines prevent overvoting through the use of interlocking mechanisms that stop a voter from pulling a lever for more candidates than

permitted (usually one) for a given office. Precinct tabulators for optical scan or even punchcard systems can detect overvotes and return the ballot uncast, thereby permitting a voter to correct the error. Of course, this feature works only if it is turned on, which has not always been the case. Tabulators can also be set to notify a voter of undervotes, but that feature is apparently rarely used because of the significant frequency of intentional undervoting. Technology that presents ballots to the voter electronically, such as DREs (direct recording electronic voting systems) and recently developed ballot-printing systems, can both prevent overvotes and indicate undervoted contests. Of course, voters can also check document ballots visually, to ensure that they have marked them completely and properly.

Differences between the Votomatic and Datavote punchcard systems illustrate some of the error-handling trade-offs involved in ballot design. A Votomatic ballot usually requires only a single card. If a voter wants to check the ballot to make sure that a vote was not missed or miscast, he or she has to find the hole that was punched out, find the corresponding number, and check that against the number in the ballot book. That must be done for each ballot item, a complex and time-consuming process. A Datavote ballot may require several cards and may need to be marked on both sides. That raises the possibility that a voter might miss a card or fail to vote on both sides. However, because the names of candidates are printed on the cards, a voter can more easily check a Datavote ballot for errors.

Voter error cannot be directly measured in elections because of the requirement for a secret ballot. Consequently, most attempts to examine voter error in the last few years have used a surrogate measure, what is often called residual votes, which is a combination of overvotes, undervotes, and spoiled ballots. This measure includes cases of voter error but also includes ballots intentionally undervoted or spoiled. Available data using this measure support the conclusion that precinct tabulation with overvote detection significantly reduces the rate of voter error involving overvotes and ballot spoilage. Recognizing this apparent benefit, HAVA requires that beginning in 2006, voting systems that use precinct tabulation provide for overvote detection. The Act does not, however, require the use of precinct tabulation, but instead stipulates that jurisdictions using central counting procedures or paper ballots (presumably meaning hand-counted paper ballots) use voter education and instruction to reduce the risk of overvotes.

Counts and Recounts. Vote counting involves several issues, including the accuracy of the counting methodology, its speed, and its integrity and security. Counting may be done in the precinct or at a central location, by machine or human inspection. With lever machines, there are no document ballots, and counts are taken at the precinct. With optical scan and punchcard systems, counts are performed electronically at the precinct or a central location, depending on the system used. In the coming election, about 80% of voters will have their votes counted electronically.

The accuracy of a vote count depends on many factors, including the characteristics of the technology used, the design and condition of the equipment and software, and human behavior. For example, since paper ballots are counted manually, the accuracy of the

count depends on the performance of the people doing the count. Lever machines reduce some kinds of human error, but problems with counts may occur as a result of malfunctioning machines or from errors made by the poll workers who read them. Punchcards and optical scan ballots are read by machine, reducing some kinds of human error, but other problems may arise from software or hardware errors, or from the ballots themselves. For example, hanging chad on a punchcard may block punched holes and be read by the counting machine as an undervote. With optical scan systems, ambiguous marks may be read differently depending on factors such as the alignment of the ballot sheet when it is fed into the tabulating machine. Problems might also arise from other sources such as software or hardware failure.

Reports on the accuracy of different systems vary. For example, some have claimed that punchcard readers can have an error rate as low as 1 vote out of each 10,000 counted under ideal test conditions. Error rates as high as 1 in 100 have been reported from prior elections, and some experts believe that Votomatic punchcard systems using prescored cards may be the least accurate of the available technologies. However, estimates from actual elections are based on residual votes and cannot distinguish errors that occur because of inherent limitations of the technology from errors or intentional actions by voters. Assessment of the accuracy of a particular voting technology should also take into account other factors, such as population size or other demographic variables. Also, the accuracy of a system in a given election may depend as well on the particular design and condition of the voting and counting equipment and the degree to which technical procedures and specifications are followed by the election personnel.

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.[3] 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.

Voting technologies may also affect recounts. With lever machines and most DREs, recounts are limited to checking the vote totals recorded by each machine. Some observers consider that an advantage because it limits the potential for human or machine error to affect the recount. Others consider it a disadvantage, because it does not allow for a ballot-by-ballot paper audit trail. With punchcard and optical scan systems, machine recounts may not produce fully repeatable results — tallies may vary slightly if recounts are repeated. Whether hand recounts are more accurate than machine counts has been the subject of considerable debate. Some observers claim that machine tabulators may miss

[3] 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%.

valid votes, misidentifying them as undervotes or overvotes, and that manual counting can detect more accurately the voter's intent. Others assert that manual counting is less objective and can create opportunities for tampering with ballots, or even that voters who fail to mark their ballots properly for machine reading should not have their ballots counted. State laws vary with respect to when manual recounts are appropriate and what standards are to be used.

All current technologies except hand-counted paper ballots can produce large counts rapidly once polls are closed. Systems in which ballots are counted electronically as they are submitted in the precinct can probably produce the most rapid results. With Votomatic systems, accuracy may be increased if the cards are manually inspected to remove loose chad before counting, but that will sacrifice some speed, and any such manipulation of cast ballots can raise questions about opportunities for tampering.

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. In fact, 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. It 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. 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, which is not available for lever machines. 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.

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, 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. 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.

Best practices. Some of the issues discussed above would require some time to address. For example, significant improvements in software and hardware can take years of work. However, other issues — including improving ballot design, reducing voter error, improving the accuracy of counts, and better security — can almost certainly be

addressed to a significant extent through improvements in practices that could be implemented for the next election. A well-designed set of recommended practices, such as the Commission is developing, could contribute significantly to such an effort. If people, process, and technology are viewed as three pillars not just of security but of successful election administration, then, given the time constraints facing the Commission, a focus on process improvements might have the greatest impact. In developing its recommendations, there are several factors the Commission might wish to consider.

The term *best practices* is often used in business and government but rarely well characterized. It often refers to strategies, policies, procedures, and other action-related elements that are generally accepted as being the most successful or cost-effective for meeting a specified set of goals. Unfortunately, there does not appear to be any overall agreement on how a best practice should be identified. Ideally, perhaps, it would involve a set of practices that were empirically and objectively demonstrated to be the best among various alternatives for achieving a stated set of goals. That is rarely achieved, and more often best practices are the result of a consensus process involving selected experts, which I understand is the approach the Commission will be taking. Such an approach can be effective, but in the absence of empirical comparisons, there is the risk of a gap between what is generally perceived to be a best practice and what in fact would be best. This risk can be mitigated in different ways, for example, by challenging participants in the consensus process to identify and examine alternatives or counterexamples.

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 possible proposal for a best practice 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, a proposed best practice intended to ensure enfranchisement would actually have the opposite effect. One solution might be for the proposed best practice to state that the

voter be informed of options and their consequences before deciding whether to vote provisionally.

Any set of proposed best practices that should be considered for adoption would likely be based on established principles — generally accepted characteristics or expectations. Relevant principles might include the following:

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.

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.

Accountability and clarity of roles. It is a standard tenet of security practice that effectiveness requires that each person involved have a clear role and that people be held appropriately accountable, according to their roles. For example, if several different people are responsible for the same task, there may be a tendency for each to assume that one of the others has done it, with the result being that it is not completed. That is especially likely when people are under severe time constraints, as often happens in busy polling places. This principle can be applied more broadly to election administration, to election officials, pollworkers, and voters.

Clear and uniform policies and procedures. A policy is essentially a set of rules governing how goals are to be met, and procedures are the actions taken to implement a policy. If either is unclear or too variable, people — pollworkers and voters — may not understand what to do in a particular situation. However, polices and procedures that are too rigid may prevent appropriate response to the kinds of unusual circumstances or special cases that often arise at the polling place.

Thorough preparation and testing. Many of the problems reported during elections are a result of voting machines or polling places that were not adequately prepared or tested before the election. Such failures appear to be especially common when significant changes to equipment and/or procedures have occurred. Where thorough preparation and testing have been performed, problems are often minimal.

Sufficient education and training of pollworkers and voters. The best policies, procedures, and technology can be for naught if the people who are to apply and use them do not understand them and are not proficient in their use and application. While the most important aspect of participation occurs at the polling place, the principle applies to all aspects of election administration.

Voter-friendly design and implementation. The importance of human engineering and usability in voting is increasingly being recognized. This principle can be applied not only to ballot design, where it has perhaps received the most attention, but also to registration, polling place layout, check-in procedures, and so forth. User-friendliness is also a potentially important factor in pollworker effectiveness and job satisfaction.

Developing a set of best practices for use in the 2004 general election is an arduous but important task. While I and my colleagues have not been able to identify sets of best practices *per se* for consideration, recommendations on practices and procedures in some of the task force reports written in the wake of the November 2000 election might be useful, in particular,

- Caltech/MIT Voting Technology Project, *Voting: What Is, What Could Be*, July 2001, a privately funded joint effort of the California Institute of Technology and the Massachusetts Institute of Technology involving faculty and staff from both institutions;
- The Constitution Project, Forum on Election Reform, *Building Consensus on Election Reform,* August 2001, from a broad-based group of organizations and experts under the auspices of a nonprofit organization focusing on legal and constitutional issues;
- National Commission on Election Standards & Reform, *Report and Recommendations to Improve America's Election System,* May 2001, from the National Association of Counties, an organization representing county governments, and the National Association of County Recorders, Election Officials, and Clerks, a professional organization of county administrative officials;
- National Conference of State Legislatures, Elections Reform Task Force, *Voting in America,* August 2001**,** from an organization serving state lawmakers; and
- National Task Force on Election Reform, *Election 2000: Review and Recommendations by the Nation's Elections Administrators,* August 2001, from The Election Center, a nonprofit organization of election administrators.

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