United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Information Policy, Census, and National Archives, House Committee on Oversight and Government Reform

For Release on Delivery
Expected at 2:00 p.m. EDT
Wednesday, April 18, 2007

ELECTIONS

All Levels of Government Are Needed to Address Electronic Voting System Challenges

Statement of Randolph C. Hite, Director
Information Technology Architecture and Systems

April 18, 2007

ELECTIONS

All Levels of Government Are Needed to Address Electronic Voting System Challenges

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-741T, a report to the Subcommittee on Information Policy, Census, and National Archives, Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

Since the 2000 national elections, concerns have been raised by various groups regarding the election process, including voting technologies. Beginning in 2001, GAO published a series of reports examining virtually every aspect of the elections process. GAO's complement of reports was used by Congress in framing the Help America Vote Act of 2002, which, among other things, provided for replacement of older voting equipment with more modern electronic voting systems and established the Election Assistance Commission (EAC) to lead the nation's election reform efforts. GAO's later reports have raised concerns about the security and reliability of these electronic voting systems, examined the EAC's efforts to address these concerns, and surveyed state and local officials about practices used during the 2004 election, as well as plans for their systems for the 2006 election.

Using its published work on electronic voting systems, GAO was asked to testify on (1) the contextual role and characteristics of electronic voting systems, (2) the range of security and reliability concerns that have been reported about these systems, (3) the experiences and management practices of states and local jurisdictions regarding these systems, and (4) the longstanding and emerging challenges facing all levels of government in using these systems.

www.gao.gov/cgi-bin/getrpt?GAO-07-741T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov.

What GAO Found

Voting systems are one facet of a multifaceted, year-round elections process that involves the interplay of people, processes, and technology, and includes all levels of government. How well these systems play their role in an election depends in large part on how well they are managed throughout their life cycles, which begins with defining system standards; includes system design, development, and testing; and concludes with system operations. Important attributes of the systems' performance are security, reliability, ease of use, and cost effectiveness.

A range of groups knowledgeable about elections or voting systems have expressed concerns about the security and reliability of electronic voting systems; these concerns can be associated with stages in the system life cycle. Examples of concerns include vague or incomplete voting system standards, system design flaws, poorly developed security controls, incorrect system configurations, inadequate testing, and poor overall security management.

For the 2004 national elections, states' and local governments' responses to our surveys showed that they did not always ensure that important life cycle and security management practices were employed for their respective electronic voting systems. In particular, responses indicated that the most current standards were not always adopted and applied, security management practices and controls were employed to varying degrees, and certain types of system testing were not commonly performed. Moreover, jurisdictions' responses showed that they did not consistently monitor the performance of their systems.

In GAO's view, the challenges faced in acquiring and operating electronic voting systems are not unlike those faced by any technology user—adoption and application of well-defined system standards; effective integration of the technology with the people who operate it and the processes that govern the operation; rigorous and disciplined performance of system security and testing activities; reliable measurement of system performance; and the analytical basis for making informed, economically justified decisions about voting system investment options. These challenges are complicated by other conditions such as the distribution of responsibilities among various organizations and funding opportunities and constraints. Given the diffused and decentralized allocation of voting system roles and responsibilities across all levels of government, addressing these challenges will require the combined efforts of all levels of government, under the leadership of the EAC. To assist the EAC in executing its leadership role, GAO has previously made recommendations to the commission aimed at better planning its ongoing and future activities relative to, for example, system standards and information sharing. While the EAC agreed with the recommendations, it stated that its ability to effectively execute its role is constrained by a lack of adequate resources.

Abbreviations

COTS commercial off-the-shelf
DRE direct recording electronic
EAC Election Assistance Commission
FEC Federal Election Commission
GSA General Services Administration
HAVA Help America Vote Act of 2002
NIST National Institute of Standards and Technology

April 18, 2007

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to participate in today's hearing on our nation's election system. As requested, my testimony will focus on our recent work on the security and reliability of electronic voting systems,[1] including the national certification and accreditation programs related to these systems and other efforts of the Election Assistance Commission (EAC).

During the 2000 national elections, concerns were raised about "hanging chads" and "butterfly ballots." In the 2004 and 2006 elections, concerns shifted to "software bugs" and "voter verifiable paper trails." In light of these and other election concerns, we produced a series of reports between 2001 and 2006 in which we examined virtually every aspect of the election process, including types of voting technology. We reported that the particular technology used to cast and count votes is a critical part of how elections are conducted, but it is only one facet of a multifaceted election process that involves the interplay of people, processes, and technology. Accordingly, we have long held the position that no voting technology, however well designed, can be a magic bullet that will solve all election problems.

My testimony today addresses four perspectives on the voting system environment: (1) the contextual role and characteristics of electronic voting systems, (2) the range of security and reliability concerns that have been reported about these systems, (3) the experiences and management practices of states and local jurisdictions regarding these systems, and (4) longstanding and emerging intergovernmental challenges in using these systems.

In preparing this testimony, we drew extensively from our published work on the election process.[2] In addition, we reviewed recent

[1]In this testimony, the term *electronic voting system* is used generically to refer to both optical scan systems and direct recording electronic systems, both of which depend on electronic technology. Each type of system is described more fully in the background section of this testimony.

[2] For example, GAO, *Elections: The Nation's Evolving Election System as Reflected in the November 2004 General Election,* GAO-06-450 (Washington, D.C.: June 6, 2006); *Elections: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be*

studies of electronic voting systems, EAC publications, and other relevant documents. All the work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

In summary, the integrity of voting systems—which is but one variable in a successful election process equation—depends on effective system life cycle management, which includes systems definition, development, acquisition, operations, testing, and management. It also depends on measuring actual voting system performance in terms of security, reliability, ease of use, and cost effectiveness, so that any needed corrective actions can be taken. Unless voting systems are properly managed throughout their life cycle, this one facet of the election process can significantly undermine the integrity of the whole.

Election officials, computer security experts, citizen advocacy groups, and others have raised significant concerns about the security and reliability of electronic voting systems, citing vague or incomplete standards, weak security controls, system design flaws, incorrect system configuration, poor security management, and inadequate security testing, among other issues. Many of these security and reliability concerns are legitimate and thus merit the combined and focused attention of federal, state, and local authorities responsible for election administration.

For the 2004 general election, states and local jurisdictions' responses to our surveys showed that they did not always use the most current voting system standards. Responses also showed that voting system practices were implemented to varying degrees and that certain types of system testing were not widely performed. Moreover, responses indicated that jurisdictions did not consistently monitor the performance of their systems. Such monitoring is important for determining where performance needs, requirements, and expectations are not being met so that corrective actions are taken.

Completed, GAO-05-956 (Washington, D.C.: Sept. 21, 2005); *Elections: Electronic Voting Offers Opportunities and Presents Challenges,* GAO-04-975T (Washington, D.C.: July 20, 2004); and *Elections: Perspectives on Activities and Challenges across the Nation,* GAO-02-3 (Washington, D.C.: Oct. 15, 2001).

The challenges confronting all levels of government in acquiring and operating voting systems for future elections are not unlike those faced by any technology user: adoption and consistent application of standards for system capabilities and performance; successful management and integration of the people, process, and technology components; rigorous and disciplined performance of testing and security activities; reliable measurement to determine whether the systems are performing as intended; and an analytical and economically justified basis for making informed decisions about voting system investment options. These challenges are heightened by other conditions common to both the national elections community and other information technology environments: the distribution of responsibilities among various organizations, technology changes, funding opportunities and constraints, emerging requirements and guidance, and public attention.

Given the diffused and decentralized allocation of voting system roles and responsibilities across all levels of government, addressing these challenges will require the combined efforts of all levels of government, under the leadership of the EAC. To assist the EAC in executing its leadership role, we previously made recommendations to the commission aimed at better planning its ongoing and future activities relative to, for example, system standards and information sharing. While the EAC agreed with the recommendations, it told us that its ability to effectively execute its role is constrained by a lack of resources. In our view, the adequacy of resources at its disposal and the degree of cooperation it receives from entities spanning all levels of government are critical elements in the commission's ability to perform its leadership role.

Background

Following the 2000 national elections, we produced a comprehensive series of reports covering our nation's election process that culminated with a capping report and framework for Congress to use to enact reforms for election administration.[3] Our reports were among the resources that Congress drew on in

[3]See, for example, GAO, *Elections: A Framework for Evaluating Reform Proposals*, GAO-02-90 (Washington, D.C.: Oct. 15, 2001).

enacting the Help America Vote Act (HAVA) of 2002,[4] which provided a framework for fundamental election administration reform and created the EAC mission to oversee the election administration reform process. HAVA also provided for funding to replace older voting equipment, specifically punch card and mechanical lever voting equipment and encouraged adoption of other technology.[5] Subsequently, jurisdictions have increased their use of electronic voting methods, of which there are two commonly-used types: optical scan and direct recording electronic (DRE).

HAVA Was Enacted to Strengthen the Overall Election Process

Enacted by Congress in October 2002, HAVA affects nearly every aspect of the voting process, from voting technology to provisional ballots and from voter registration to poll worker training. In particular, the act authorized $3.86 billion in funding over several fiscal years for programs to replace punch card and mechanical lever voting equipment, improve election administration and accessibility, train poll workers, and perform research and pilot studies. HAVA also established the EAC to assist in the administration of federal elections and provide assistance with the administration of certain federal election laws and programs. HAVA also established minimum election administration standards for the states and units of local government that are responsible for the administration of federal elections. The act specifically tasked the EAC to serve as a national clearinghouse and resource for compiling election information and reviewing election procedures; for example, it is to conduct periodic studies of election administration issues, including electronic voting system performance, to promote methods of voting and administration that are most convenient, accessible, and easy to use for all voters. Other examples of EAC responsibilities include

- developing and adopting voluntary voting system guidelines and maintaining information on the experiences of states in implementing the guidelines and operating voting systems;

[4]Help America Vote Act of 2002, Pub. L. No. 107-252 (Oct. 29, 2002).
[5]The General Services Administration (GSA) is responsible for administering grants to the states to replace punch card systems and lever machines in qualifying states, including providing payments for general election administration improvements to states that apply for funds to replace voting equipment.

- testing, certifying, decertifying, and recertifying voting system hardware and software through accredited laboratories;
- making payments to states to help them improve elections in the areas of voting systems standards, provisional voting and voting information requirements, and computerized statewide voter registration lists; and
- making grants for research on voting technology improvements.

The act also established the Technical Guidelines Development Committee to support the EAC, making it responsible for recommending voluntary voting system guidelines to the EAC. The act assigned the National Institute of Standards and Technology (NIST) responsibility for providing technical support to the development committee and made the NIST Director the committee chair.

The EAC began operations in January 2004, initially focusing on the distribution of funds to help states meet HAVA's Title III requirements for uniform and nondiscriminatory election technology and administration, including the act's requirements pertaining to voting system standards, provisional voting, voting information, a computerized statewide voter registration list, and identification for first-time voters who register to vote by mail. Actions EAC has taken since 2004 to improve voting systems include

- publishing the *Best Practices Toolkit* and specialized management guides to assist states and local jurisdictions with managing election-related activities and equipment;
- issuing voting system standards in 2005, referred to as the *Voluntary Voting System Guidelines*;
- establishing procedures for certifying voting systems;
- establishing a program for accreditation of independent testing laboratories, with support from NIST's National Voluntary Laboratory Accreditation Program;
- disbursing to states approximately $2.3 billion in appropriations for the replacement of older voting equipment and election administration improvements under Title III of HAVA; and

- conducting national surveys of the 2004 general election, uniformed and overseas voters, and other studies.

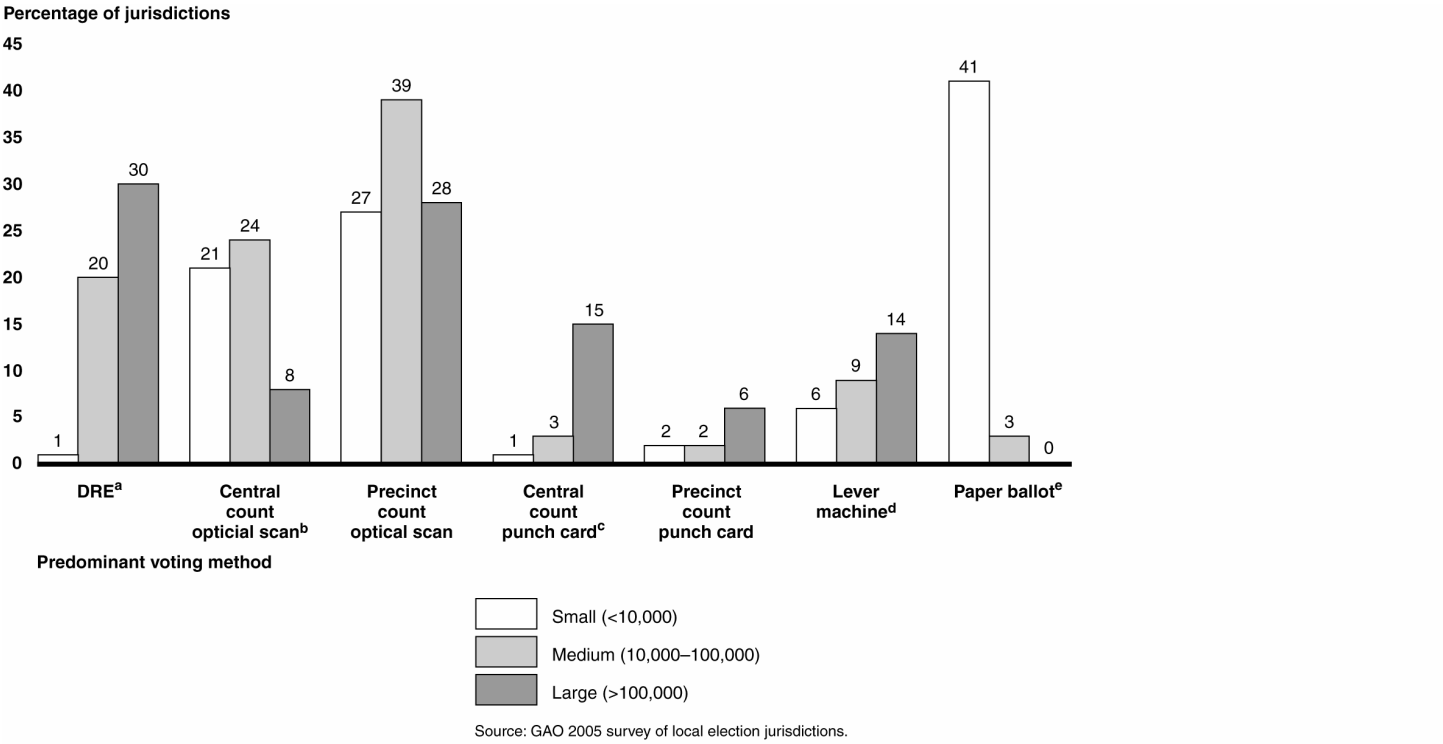
For fiscal year 2006, EAC's appropriation totaled $14.1 million. EAC reported that this included $3.8 million (27 percent) for activities related to development and adoption of the voting system standards and the voting system certification program; $3.5 million (25 percent) for research and study and to establish the EAC as a national clearinghouse of election administration information; and $2.8 million (20 percent) to manage HAVA funds distributed to the states. The remaining funds went to various administrative expenses, including funding various advisory board meetings. EAC's budget for fiscal year 2007 is $16.91 million, of which $4.95 million (29 percent) is to be transferred to NIST for its work on voting system standards and research performed under HAVA. EAC's requested budget for fiscal year 2008 is $15.5 million, of which $3.25 million (21 percent) is to be transferred to NIST.

Electronic Voting Systems Fall into Two Primary Categories

In the United States today, most votes are cast and counted by one of two types of electronic voting systems: optical scan and direct recording electronic (DRE). For the November 2004 general election, optical scan was the predominant voting method for more than half of local jurisdictions nationwide. In contrast, DREs were used as the predominant voting method by an estimated 7 percent of jurisdictions, although they were the predominant voting method for large jurisdictions.[6] Figure 1 shows the estimated percentage of small, medium, and large jurisdictions using each predominant voting method in the 2004 general election.

[6]To obtain national information from local election officials on changes to election systems since 2000, election administration, and their experiences in the 2004 general election, we conducted a mail survey of a stratified random probability sample of 788 local election jurisdictions nationwide. Unless otherwise noted, the maximum sampling error at the 95 percent level of statistical confidence for estimates from this survey of all jurisdictions is plus or minus 5 percentage points, plus or minus 7 percentage points for large jurisdictions, plus or minus 7 percentage points for medium population size jurisdiction, and plus or minus 5 percentage points for small population size jurisdictions. For more details about this survey, see appendix V in GAO-06-450.

Figure 1: Estimated Percentage of Jurisdictions Using Predominant Voting Methods in 2004, by Jurisdiction Size



Source: GAO 2005 survey of local election jurisdictions.

Note: Percentages for predominant voting methods within each jurisdiction size may not add to 100 because of rounding.
[a]The differences between small jurisdictions and both medium and large jurisdictions are statistically significant.
[b]The differences between both small and medium jurisdictions and large jurisdictions are statistically significant.
[c]The differences between both small and medium jurisdictions and large jurisdictions are statistically significant.
[d]The difference between small jurisdictions and large jurisdictions is statistically significant.
[e]The differences between small jurisdictions and both medium and large jurisdictions are statistically significant.

Optical Scan Systems

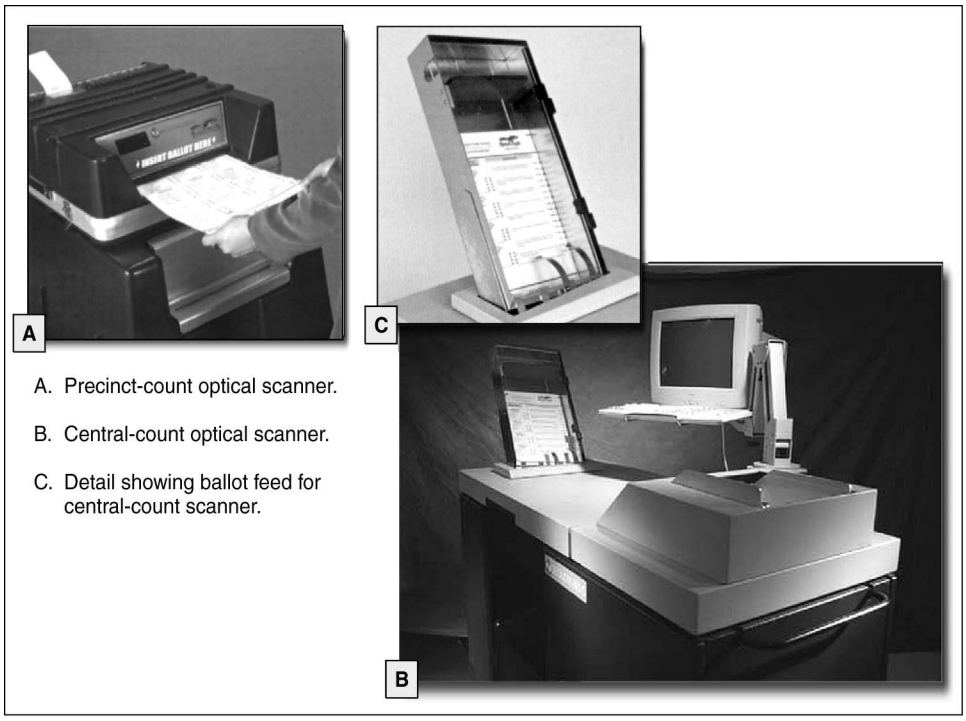
Optical scan voting systems use electronic technology to tabulate paper ballots. For the 2004 general election, we estimated that about 51 percent of all local jurisdictions used optical scan voting equipment predominantly.

An optical scan voting system is made up of computer-readable ballots, appropriate marking devices, privacy booths, and a computerized tabulation device. The ballot, which can be of various sizes, lists the names of the candidates and the issues. Voters record their choices using an appropriate writing instrument to fill in boxes or ovals or to complete an arrow next to the candidate's name or the issue. The ballot includes a space for write-ins to be placed directly on the ballot.

Optical scan ballots are tabulated by optical-mark-recognition equipment (see fig. 2), which counts the ballots by sensing, or reading, the marks on the ballot. Ballots can be counted at the polling place—this is referred to as precinct-count optical scan[7]—or at a central location. If ballots are counted at the polling place, voters or election officials put the ballots into the tabulation equipment, which tallies the votes; these tallies can be captured in removable storage media that are transported to a central tally location, or they can be electronically transmitted from the polling place to the central tally location. If ballots are centrally counted, voters drop ballots into sealed boxes and election officials transfer the sealed boxes to the central location after the polls close, where election officials run the ballots through the tabulation equipment.

[7]Precinct-count optical scan equipment sits on a ballot box with two compartments for scanned ballots—one for accepted ballots (i.e., those that are properly filled out) and one for rejected ballots (i.e., blank ballots, ballots with write-ins, or those accepted because of a forced override). In addition, an auxiliary compartment in the ballot box is used for storing ballots if an emergency arises (e.g., loss of power or machine failure) that prevents the ballots from being scanned.

Figure 2: Precinct-Count Optical Scan Tabulator and Central-Count Optical Scan Tabulator



Source: Equipment vendors.

Software instructs the tabulation equipment to assign each vote (i.e., to assign valid marks on the ballot to the proper candidate or issue). In addition to identifying the particular contests and candidates, the software can be configured to capture, for example, straight party voting and vote-for-no-more-than-N contests. Precinct-based optical scanners can also be programmed to detect overvotes (where the voter, for example, votes for two candidates for one office, invalidating the vote) and undervotes (where the voter does not vote for all contests or issues on the ballot) and to take some action in response (rejecting the ballot, for instance), so that voters can fix their mistakes before leaving the polling place. If ballots are tabulated centrally, voters do not have the opportunity to detect and correct mistakes that may have been made. In addition, optical scan systems often use vote tally software to tally the vote totals from one or more vote tabulation devices.

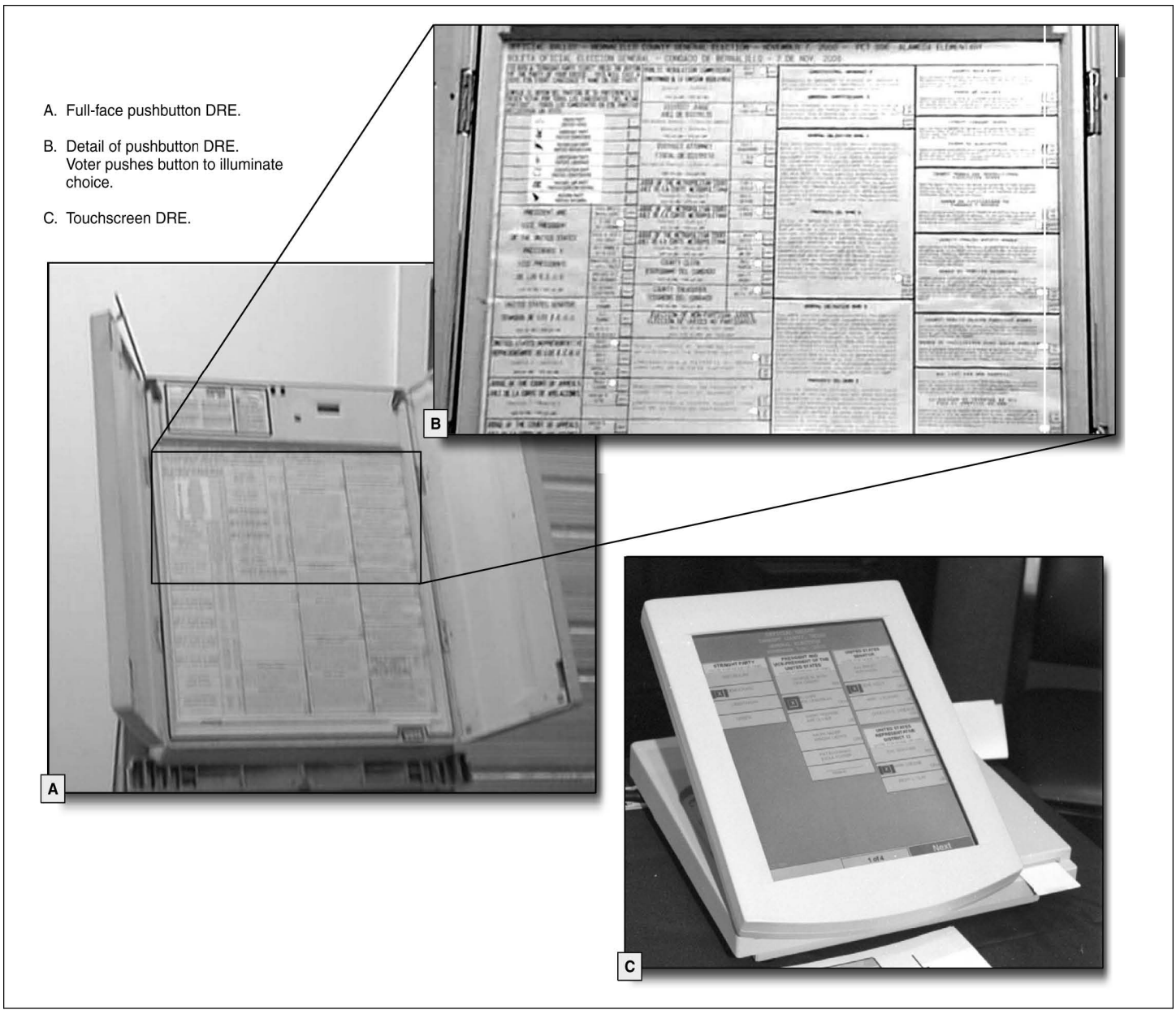
Optical scan systems were widely used as the predominant voting method for jurisdictions in the 2004 general election and we reported last year that jurisdictions planned to acquire more of these systems for the 2006 general election. We estimated that 30 percent of jurisdictions nationwide used precinct count optical scan voting equipment as their predominant voting method for the 2004 general election, while an estimated 21 percent used central count optical scan predominantly. While all sizes of jurisdictions had plans to acquire both precinct count and central count optical scan systems for the 2006 general election, small jurisdictions showed a strong preference for acquiring precinct count optical scan systems (estimated at 28 percent of small jurisdictions) compared with DREs (13 percent) and central count optical scan (4 percent).

Direct Recording Electronic Systems

DREs capture votes electronically without the use of paper ballots. For the 2004 general election, we estimated that about 7 percent of all local jurisdictions used DREs predominantly, although 30 percent of all large jurisdictions used them as the predominant voting method.

DREs come in two basic types: pushbutton or touch screen, with pushbutton being the older technology. The two types vary considerably in appearance, as shown in figure 3.

Figure 3: DRE Pushbutton and DRE Touch Screen



Source: Local election officials and equipment vendor.

Pushbutton and touch screen units differ significantly in the way they present ballots to the voter. With the pushbutton type, all ballot information is presented on a single "full-face" ballot. For example,

a ballot may have 50 buttons on a 3 by 3 foot ballot, with a candidate or issue next to each button. In contrast, touch screen DREs display ballot information on an electronic display screen. For both pushbutton and touch screen types, the ballot information is programmed onto an electronic storage medium, which is then uploaded to the machine. For touch screens, ballot information can be displayed in color and can incorporate pictures of the candidates. Because the ballot space on a touch screen is much smaller than on a pushbutton machine, voters who use touch screens must page through the ballot information. Both touch screen and pushbutton DREs can accommodate multilingual ballots.

Despite the differences between pushbutton and touch screen DREs, the two types have some similarities, such as how the voter interacts with the voting equipment. To make a ballot selection, voters press a button or the screen next to the candidate or issue, and the button or screen then lights up to indicate the selection. When voters are finished making their selections, they cast their votes by pressing a final "vote" button or screen. Until they hit this final button or screen, voters can change their selections. DREs are designed to not allow overvotes. Both types allow voters to write in candidates. While most DREs allow voters to type write-ins on a keyboard, some pushbutton types require voters to write the name on paper tape that is part of the device. In addition, different types of DREs offer a variety of options that jurisdictions may choose to purchase, such as printed receipts or audio interfaces for voters with disabilities.

Although DREs do not receive paper ballots, they can retain permanent electronic images of all the ballots, which can be stored on various media, including internal hard disk drives, flash cards, or memory cartridges. According to vendors, these ballot images, which can be printed, can be used for auditing and recounts.

Like optical scan devices, DREs require the use of software to program the various ballot styles and tally the votes, which is generally done through the use of memory cartridges or other media. Some of the newer DREs use smart card technology as a security feature. Smart cards are plastic devices—about the size of a credit card—that use integrated circuit chips to store and process data, much like a computer. Smart cards are generally used as a

means to open polls and to authorize voter access to ballots. For instance, smart cards on some DREs store program data on the election and are used to help set up the equipment; during setup, election workers verify that the card received is for the proper election. Other DREs are programmed to automatically activate when the voter inserts a smart card; the card brings up the correct ballot onto the screen.

DREs offer various configurations for tallying the votes. Some contain removable storage media that can be taken from the voting device and transported to a central location to be tallied. Others can be configured to electronically transmit the vote totals from the polling place to a central tally location. Vote tally software is often used to tally the vote totals from one or more units.

DREs were chosen as the predominant voting method by a relatively small overall proportion of local jurisdictions for the 2004 general election (7 percent overall). However, as previously shown in figure 1, large and medium jurisdictions identified DREs as their predominant voting method (estimated at 30 percent and 20 percent of jurisdictions, respectively) more often than small jurisdictions (estimated at 1 percent). DREs were the leading choice among voting methods for both large and medium jurisdictions that planned to acquire voting systems before the 2006 general election (an estimated 34 percent of jurisdictions in both size groups).

Contextual Role and Performance Characteristics of Electronic Voting Systems Are Important to Understanding Their Use

Voting systems are one facet of a multifaceted, continuous elections process that involves the interplay of people, processes, and technology. All levels of government—federal, state, and local—share responsibilities for aspects of elections and voting systems. Moreover, effective performance of these systems is a product of effective system life cycle management, which includes systems definition, development, acquisition, operations, testing, and management. Such performance can be viewed in terms of several characteristics, such as security, reliability, ease of use, and cost effectiveness.

Despite Their Vital Role, Voting Systems Are Only One Aspect of the Larger Election Process

Voting systems represent one of many important components in the overall election process. This process involves all levels of government and is made up of several stages, with each stage consisting of the interplay of people, processes, and technology.

At the federal level, Congress has authority under the Constitution to regulate the administration of presidential and congressional elections and to enforce prohibitions against specific discriminatory practices in all elections—federal, state, and local.[8] It has passed legislation affecting the administration of state elections that addresses voter registration,[9] absentee voting,[10] accessibility provisions for the elderly and handicapped,[11] and prohibitions against discriminatory practices.[12] Congress does not have general constitutional authority over the administration of state and local elections.

At the state level, the states are responsible for the administration of both their own elections and federal elections. States regulate the election process, including, for example, adoption of voting system standards, testing of voting systems, ballot access, registration procedures, absentee voting requirements, establishment of voting locations, provision of Election Day workers, and counting and certification of the vote. As we have reported, the U.S. election process can be seen as an assemblage of 51 somewhat distinct election systems—those of the 50 states and of the District of Columbia.

Further, although election policy and procedures are legislated primarily at the state level, states typically have decentralized this

[8]For more information on the role of the federal government in the administration of elections, see GAO, *Elections: The Scope of Congressional Authority in Election Administration*, GAO- 01-470 (Washington, D.C.: Mar. 13, 2001).
[9]National Voter Registration Act of 1993, commonly known as the "Motor Voter" Act; 42 U.S.C. 1973gg to 1973gg-10.
[10]Uniformed and Overseas Citizens Absentee Voting Act (1986); 42 U.S.C. 1973ff to 1973ff-6.
[11]Voting Accessibility for the Elderly and Handicapped Act (1984); 42 U.S.C. 1973ee to 1973ee-6.
[12]Voting Rights Act of 1965, 42 U.S.C. 1973 to 1973bb-1.

process so that the details of administering elections are carried out at the city or county levels, and voting is done at the local level. This is important because local election jurisdictions number more than 10,000 and their size varies enormously—from a rural county with about 200 voters to a large urban county such as Los Angeles County, where the total number of registered voters for the 2000 elections exceeded the registered voter totals in 41 states.

The size and demographics of a voting jurisdiction significantly affects the complexity of planning and conducting the election, as does the method used to cast and count votes. For example, jurisdictions using DRE systems may need to manage the electronic transmission of votes or vote counts, while jurisdictions using optical scan technology need to manage the transfer of the paper ballots this technology reads and tabulates. Jurisdictions using optical scan technology may also need to manage electronic transmissions if votes are counted at various locations and totals are electronically transmitted to a central tally point. No matter what technology is used, jurisdictions may need to provide ballot translations; however, the logistics of printing paper materials in a range of languages, as would be required for optical scan technology, is different from the logistics of programming translations into DRE units.

Some states do have statewide election systems so that every voting jurisdiction uses similar processes and equipment, but others do not. For instance, we reported in 2001 that in Pennsylvania, local election officials told us that there were 67 counties and consequently 67 different ways of handling elections.[13] In some states, such as Georgia, state law prescribes the use of common voting technology throughout the state while in other states, local election officials generally choose the voting technology to be used in their precincts, often from a list of state-certified options.

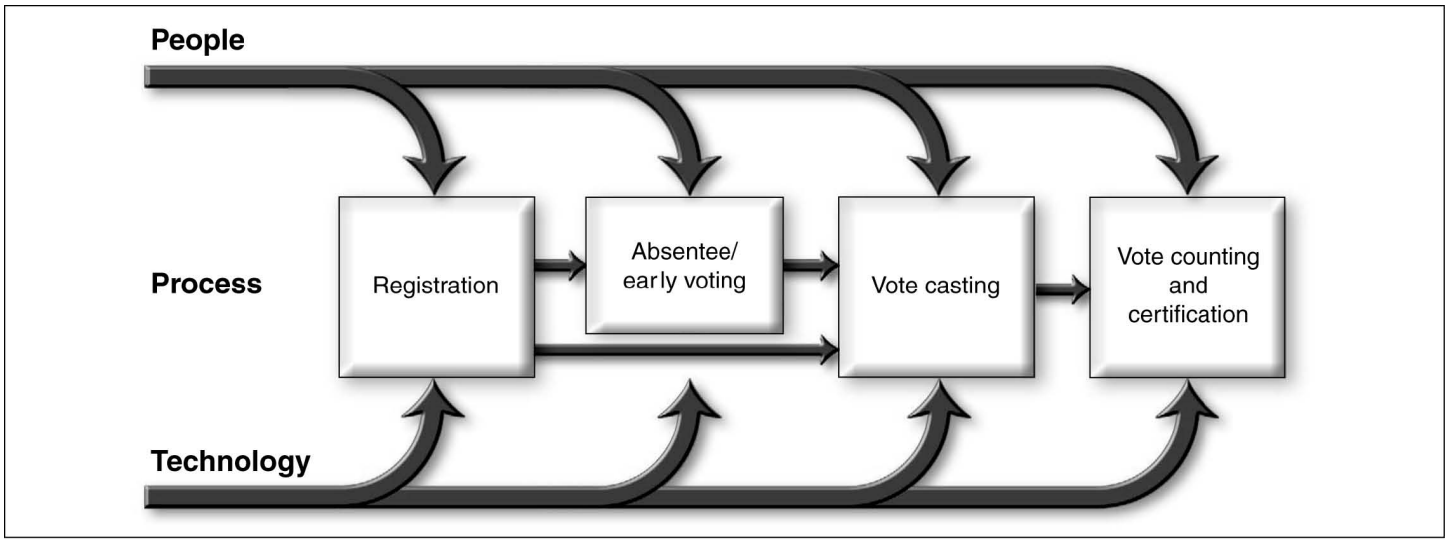
Regardless of levels of government, however, election administration is a year-round activity, involving varying sets of people performing the activities of each stage of the election process. These stages generally consist of the following:

[13]GAO-02-3.

- **Voter registration.** Among other things, local election officials register eligible voters and maintain voter registration lists, including updates to registrants' information and deletions of the names of registrants who are no longer eligible to vote.
- **Absentee and early voting.** This type of voting allows eligible persons to vote in person or by mail before Election Day. Election officials must design ballots and other systems to permit this type of voting and educate voters on how to vote by these methods.
- **Election Day vote casting.** Election administration includes preparation before Election Day, such as local election officials arranging for polling places, recruiting and training poll workers, designing ballots, and preparing and testing voting equipment for use in casting and tabulating votes, as well as Election Day activities, such as opening and closing polling places and assisting voters in casting their votes.
- **Vote counting.** At this stage, election officials tabulate the cast ballots, determine whether and how to count ballots that cannot be read by the vote counting equipment, certify the final vote counts, and perform recounts, if required.

As shown in figure 4, each stage of an election involves people, processes, and technology.

Figure 4: Stages of Election Process



Source: GAO analysis.

Electronic voting systems are primarily involved in the last three stages, during which votes are recorded, cast, and counted. However, the type of system that a jurisdiction uses may affect earlier stages. For example, in a jurisdiction that uses optical scan systems, paper ballots like those used on Election Day may be mailed in the absentee voting stage. On the other hand, a jurisdiction that uses DRE technology would have to make a different provision for absentee voting.

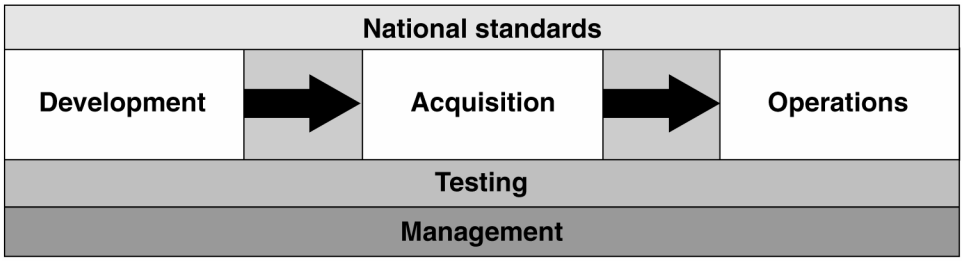
Management of Electronic Voting System Performance Is a Continuous Process

The performance of any information technology system, including electronic voting systems, is heavily influenced by a number of factors, including how well the system is defined, developed, acquired, tested, and implemented.

Like any information technology product, a voting system starts with the explicit definition of what the system is to do and how well it is to do it. These requirements are then translated into design specifications that are used to develop the system. Electronic voting systems are typically developed by vendors and then purchased as commercial off-the-shelf (COTS) products and implemented by state and local election administrators. During the development,

acquisition, and implementation of the systems, a range of tests are performed and the process is managed to ensure performance expectations are met. Together, these activities form a voting system life cycle (see fig. 5).

Figure 5: Simplified Voting System Life Cycle



Sources: GAO analysis of NIST, IEEE, and EAC publications.

Unless voting systems are properly managed throughout their life cycle, this one facet of the election process can significantly undermine the integrity of the whole.

Standards. Voting system standards define the functional and performance requirements that must be met and thus provide the baseline against which systems can be developed and tested. They also specify how the systems should be implemented and operated. Voting system standards apply to system hardware, software, firmware, and documentation, and they span prevoting,voting, and postvoting activities. They address, for example, requirements relating to system security; system reliability (accuracy and availability); system auditability; system storage and maintenance; and data retention and transportation. In addition to national standards, some states and local jurisdictions have specified their own voting system requirements.

Development. Product development is performed by the voting system vendor. Product development includes further establishing system requirements, designing the system architecture, developing software, integrating hardware and software components, and testing the system.

Acquisition. Voting system acquisition activities are performed by state and local governments and include publishing a request for proposals, evaluating proposals, choosing a voting system method,

choosing a vendor, writing and administering contracts, and testing the acquired system.

Operations. Operation of voting systems is typically the responsibility of local jurisdictions. These activities include setting up systems before voting, vote capture and counting during elections, recounts and system audits after elections, and storage of systems between elections. Among other things, this phase includes activities associated with the physical environments in which the system operates. These include ensuring the physical security of the polling place and voting equipment and controlling the chain of custody for voting system components and supplies. The operations phase also includes monitoring of the election process by use of system audit logs and backups, and the collection, analysis, reporting, and resolution of election problems.

Testing. As noted, testing is conducted by multiple entities throughout the life cycle of a voting system. Voting system vendors conduct testing during system development. National testing of systems is conducted by accredited independent testing authorities. Some states conduct testing before acquiring a system to determine how well it meets the specified performance parameters, or states may conduct certification testing to ensure that a system performs as specified by applicable laws and requirements. Once a voting system is delivered by the vendor, states and local jurisdictions may conduct acceptance testing to ensure that the system satisfies requirements. Finally, local jurisdictions typically conduct logic and accuracy tests prior to each election and sometimes subject portions of the system to parallel testing during each election.

Management. Management processes ensure that each life cycle phase produces desirable outcomes and is conducted by the organization responsible for each life cycle phase. Voting system vendors manage the development phase, while states and/or local jurisdictions manage the acquisition and operations phases. Typical management activities that span the system life cycle include planning, configuration management, system performance review and evaluation, problem tracking and correction, human capital management, and user training. Management responsibilities related to security and reliability include program planning, disaster recovery and contingency planning, definition of security roles and

responsibilities, configuration management of voting system hardware and software, and poll worker security training.

Electronic Voting System Performance Can Be Judged on Several Attributes

Although the debate concerning electronic voting systems is primarily focused on security, other performance attributes are also relevant, such as reliability, ease of use, and cost. Each of these attributes is described here.

Security. Election officials are responsible for establishing and managing security and privacy controls to protect against threats to the integrity of elections.[14] Threats to election results and voter confidentiality include potential modification or loss of electronic voting data; loss, theft, or modification of physical ballots; and unauthorized access to software and electronic equipment. Different types of controls can be used to counter these threats. Physical access controls are important for securing voting equipment, vote tabulation equipment, and ballots. Software access controls (such as passwords and firewalls[15]) are important for limiting the number of people who can access and operate voting devices, election management software, and vote tabulation software. In addition, physical screens around voting stations and poll workers preventing voters from being watched or coerced while voting are important to protect the privacy and confidentiality of the vote.

Reliability. Ensuring the reliability of votes being recorded and tallied is an essential attribute of any voting equipment and depends to a large degree on the accuracy and availability of voting systems. Without such assurance, both voter confidence in the election and the integrity and legitimacy of the outcome of the election are at risk. The importance of an accurate vote count increases with the

[14]We have described an effective security program as including, at a minimum, (1) assigning responsibility for security, (2) assessing security risks and vulnerabilities and implementing both manual and technology-based security measures to prevent or counter these risks, and (3) periodically reviewing the controls to ensure their appropriateness. For more information, see GAO, *Executive Guide: Information Security Management*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

[15]A firewall is a hardware or software component that protects computers or networks from attacks by outside network users by blocking and checking all incoming traffic.

closeness of the election. Both optical scan and DRE systems are claimed to be highly accurate. Although voting equipment may be designed and developed to count votes as recorded with 100 percent accuracy, how well the equipment counts votes as intended by voters is a function not only of equipment design, but also of how procedures are followed by election officials, technicians, and voters. It is also important to limit system down time so that polling places can handle the volume of voter traffic.

Ease of Use. Ease of use (or user friendliness) depends largely on how voters interact physically and intellectually with the voting system. This interaction, commonly referred to as the human/machine interface, is a function of the system design and how it has been implemented. Ease of use depends on how well jurisdictions design ballots and educate voters on the use of the equipment. A voting system's ease of use affects accuracy (i.e., whether the voter's intent is captured), and it can also affect the efficiency of the voting process (confused voters take longer to vote). Accessibility by diverse types of voters, including those with disabilities, is a further aspect of ease of use.

Cost. For a given jurisdiction, the particular cost associated with an electronic voting system will depend on the requirements of the jurisdiction as well as the particular equipment chosen. Voting equipment costs vary among types of voting equipment and among different manufacturers and models of the same type of equipment. Some of these differences can be attributed to differences in what is included in the unit cost. In addition to the equipment unit cost, an additional cost for jurisdictions is the software that operates the equipment, prepares the ballots, and tallies the votes (and in some cases, prepares the election results reports). Other factors affecting the acquisition cost of voting equipment are the number and types of peripherals required. Once jurisdictions acquire the voting equipment, they also incur the cost to operate and maintain it, which can vary considerably.

Widespread Concerns about Electronic Voting Systems Have Been Reported

Election officials, computer security experts, citizen advocacy groups, and others have raised significant security and reliability concerns with electronic voting systems, citing, for example, inadequacies in standards, system design and development, operation and management activities, and testing. In 2005, we examined the range of concerns raised by these groups and aligned them with their relevant life cycle phases. We also examined EAC's efforts related to these concerns. Furthermore, we identified key practices that each level of government should implement throughout the voting system life cycle in order to improve security and reliability.[16]

The aspects of the voting system life cycle phases are interdependent—that is, a problem experienced in one area of the life cycle will likely affect other areas. For example, a weakness in system standards could result in a poorly designed and developed system, which may not perform properly in the operational phase. State and local jurisdictions have documented instances when their electronic voting systems exhibited operational problems during elections. Such failures led to polling place delays, disruptions, and incorrect vote tabulations.

In reviewing the reported concerns, we have explained that many of the security and reliability concerns involved vulnerabilities or problems with specific voting system makes and models or unique circumstances in a specific jurisdiction's election, and there is a lack of consensus among elections officials, computer security experts, and others on the pervasiveness of the concerns. We concluded in 2005 that these concerns have caused problems with recent elections, resulting in the loss and miscount of votes. In light of the demonstrated voting system problems; the differing views on how widespread these problems are; and the complexity of assuring the accuracy, integrity, confidentiality, and availability of voting systems throughout their life cycles, we stated that the security and

[16]GAO-05-956.

reliability concerns merit the focused attention of federal, state, and local authorities responsible for election administration.

Inadequate National Standards

Appropriately defined and implemented standards for system functions and testing processes are essential to ensuring the security and reliability of voting systems across all phases of the elections process. States and local jurisdictions face the challenge of adapting to and consistently applying appropriate standards and guidance to address vulnerabilities and risks in their specific election environments. The national standards are voluntary—meaning that states are free to adopt them in whole or in part or reject them entirely.

The Federal Election Commission (FEC) issued a set of voluntary voting system standards in 1990 and revised them in 2002. These standards identify requirements for electronic voting systems. Computer security experts and others criticized the 2002 voting system standards for not containing requirements sufficient to ensure secure and reliable voting systems. Common concerns with the standards involved their vague and incomplete security provisions, inadequate provisions for some commercial products and networks, and inadequate documentation requirements.

In December 2005, EAC issued the *Voluntary Voting System Guidelines*, which includes additions and revisions for system functional requirements, performance characteristics, documentation requirements, and test evaluation criteria for the national certification of voting systems. These guidelines promote security measures that address gaps in prior standards and are applicable to more modern technologies, such as controls for software distribution and wireless operations.

As we previously reported, the 2005 *Voluntary Voting System Guidelines* do not take effect until December 2007. Moreover, this version of the standards does not comprehensively address voting technology issues. For instance, they do not address COTS devices (such as card readers, printers, or personal computers) or software products (such as operating systems or database management systems) that are used in voting systems without modification. This is significant because computer security experts have raised

concerns about a provision in the prior voting system standards that exempted unaltered COTS software from testing and about voting system standards that are not sufficient to address the weaknesses inherent in telecommunications and networking services. Specifically, vendors often use COTS software in their electronic voting systems, including operating systems. Security experts note that COTS software could contain defects, vulnerabilities, and other weaknesses that could be carried over into electronic voting systems, thereby compromising their security. Regarding telecommunications and networking services, selected computer security experts believe that relying on any use of telecommunications or networking services, including wireless communications, exposes electronic voting systems to risks that make it difficult to adequately ensure their security and reliability—even with safeguards such as encryption and digital signatures in place.

As states and jurisdictions move to a more integrated suite of election systems, proactive efforts to establish standards in such areas will be essential to addressing emerging technical, security, and reliability interactions among systems and managing risks in this dynamic election environment. However, the 2005 guidelines do not address the emerging trends in election systems, such as the integration of registration systems with voting systems.

In light of this and other weaknesses in the standards, we reported in 2005 that EAC did not yet have detailed plans in place for addressing these deficiencies. Accordingly, we recommended that EAC collaborate with NIST and the Technical Guidelines Development Committee to define specific tasks, measurable outcomes, milestones, and resource needs required to improve the standards. To its credit, EAC agreed with our recommendation, recognizing that more work was needed to further develop the technical guidelines. Accordingly, it stated that it planned to work with NIST to plan and prioritize its standards work within its scarce resources.

Inadequate System Design and Development

Multiple reports, including several state-commissioned technical reviews and security assessments, have raised concerns about the

design and development of secure and reliable electronic voting systems. Among other things, weak embedded security controls and audit trail design flaws were two major areas of concern:

- **Weak system security controls.** Some electronic voting systems reportedly have weak software and hardware security controls. Regarding software controls, many security examinations reported flaws in how controls were implemented in some DRE systems to prevent unauthorized access. For example, one model failed to password-protect the supervisor functions controlling key system capabilities; another relied on an easily guessed password to access these functions. If exploited, these weaknesses could damage the integrity of ballots, votes, and voting system software by allowing unauthorized modifications. Regarding physical hardware controls, several recent reports found that certain DRE models contained weaknesses in controls designed to protect the system. For instance, reviewers were concerned that a particular model of DRE was set up in such a way that if one machine was accidentally or intentionally unplugged from the others, voting functions on the other machines in the network would be disrupted. In addition, reviewers found that the switches used to turn a DRE system on or off, as well as those used to close the polls on a particular DRE terminal, were not protected.

- **Design flaws in developing voter-verified paper audit trails.** Establishing a voter-verified paper audit trail involves adding a paper printout to a DRE system so that a voter can review and verify his or her ballot. Some citizen advocacy groups, security experts, and elections officials advocate these audit trails as a protection against potential DRE flaws. However, other election officials and researchers have raised concerns about potential reliability and security flaws in the design of systems using voter-verified paper audit trails. If voting system mechanisms for protecting the paper audit trail were inadequate, an insider could associate voters with their individual paper ballots and votes, particularly if the system stored voter-verified ballots sequentially on a continuous roll of paper. If not protected, such information could breach voter privacy and confidentiality.

Inadequate System Operation and Management Activities

Several reports raised concerns about the operational practices of local jurisdictions and the actual performance of their respective electronic voting systems during elections. These include incorrect system configurations, inadequate security management programs, and poor implementation of security procedures.

- **Incorrect system configuration.** Some state and local election reviews have documented cases in which local governments did not properly configure their voting systems. These improper configurations resulted in voters being unable to vote in certain races or their votes not being captured correctly by the voting system.

- **Poor version control of system software.** Security experts and some election officials expressed concern that the voting system software installed at the local level may not be the same as what was qualified and certified at the national or state levels. These groups raised the possibilities that either intentionally or by accident, voting system software could be altered or substituted, or that vendors or local officials might install untested or uncertified versions of voting systems, knowingly or unknowingly. As a result, potentially unreliable or malicious software might be used in elections.

- **Inadequate security management programs.** Several technical reviews found that states did not have effective information security management plans in place to oversee their electronic voting systems. The reports noted that key managerial functions were not in place, including (1) providing appropriate security training, (2) ensuring that employees and contractors had proper certifications, (3) ensuring that security roles were well defined and staffed, and (4) ensuring that pertinent officials correctly set up their voting system audit logs and require them to be reviewed.

- **Poor implementation of security procedures.** Several reports indicated that state and local officials did not always follow security procedures. For example, reports found that a

regional vote tabulation computer was connected to the Internet and that local officials had not updated it with several security patches, thus needlessly exposing the system to security threats. In addition, several reports indicated that some state and local jurisdictions did not always have procedures in place to detect problems with their electronic voting systems such as ensuring the number of votes cast matched the number of signatures on precinct sign-in sheets.

Inadequate Testing

Security experts and some election officials have expressed concerns that the tests performed by independent testing authorities and state and local election officials do not adequately assess electronic voting systems' security and reliability. These concerns are intensified by what some perceive as a lack of transparency in the testing process.

- **Inadequate security testing.** Many computer security experts expressed concerns with weak or insufficient system testing, source code reviews, and penetration testing. To illustrate their concerns, they pointed to the fact that most of the systems that exhibited the weak security controls previously cited had been nationally certified after testing by an independent testing authority. Security experts and others point to this as an indication that both the standards and the testing program are not rigorous enough with respect to security.

- **Lack of transparency in the testing process.** Security experts and some elections officials have raised concerns about a lack of transparency in the testing process. They note that the test plans used by the independent testing authorities, along with the test results, are treated as protected trade secrets and thus cannot be released to the public. Critics say that this lack of transparency hinders oversight and auditing of the testing process. This in turn makes it harder to determine the actual capabilities, potential vulnerabilities, and performance problems of a given system. Despite assertions by election officials and vendors that disclosing too much information about an electronic voting system could pose a security risk, one security

expert noted that a system should be secure enough to resist even a knowledgeable attacker.

Variability and Weaknesses in State and Local Approaches to Voting System Standards, Testing, Operations, and Performance Measurement

In 2006, we reported on state and local government experiences in conducting the 2004 national election.[17] Regarding voting systems, states' and jurisdictions' responses to our surveys showed that differing versions of the national voting system standards were used (not always the most current version); voting system life cycle management practices were not consistently implemented; and certain types of system testing were not widely performed. Moreover, jurisdictions reported that they did not consistently monitor the performance of their systems, which is important for determining whether election needs, requirements, and expectations are met and for taking corrective actions when they are not.

States' Use of Standards Varied

States and jurisdictions reported that they applied a variety of voting system standards, some of which were no longer current. Specifically, 44 states and the District of Columbia reported that they were requiring local jurisdictions' voting systems to be used for the first time in the November 2006 general election to comply with the national voting system standards.[18] However, these states were not all using the same version of the standards. This is troublesome because the later versions of the standards are more stringent than the earlier versions in various areas, including security.

More specifically, 28 of the 44 states and the District of Columbia reported that voting systems to be used for the first time in the 2006

[17]GAO-06-450.

[18]To obtain information from state election officials on any changes made in selected state statutory requirements since the 2000 election and other changes made including actions taken to implement HAVA, we conducted a Web-based survey of the 50 states and the District of Columbia. For more details about this survey, see appendix V in GAO-06-450.

election comply with the 2002 voting system standards. Nine of these 28 states would also require their jurisdictions to apply the 1990 federal standards to new voting systems and 4 of the 28 would also require jurisdictions to use the 2005 voting system standards, which were in draft version at the time of our survey. (One other state also expected to apply the 2005 voting system standards.) Ten other of the 44 states reporting said that they expected to use hybrid standards that were based on one or more versions of the national standards, without specifying the composition of their hybrid, and 4 states planned to use the national standards in 2006, but did not specify a version. (Five states responded that they did not require their voting systems to comply with any version of the national standards or had not yet made a decision on compliance with the standards for 2006. One state did not respond.)

Jurisdictions Varied Widely in Applying Security Practices

Local jurisdictions varied widely in the nature and extent of their voting system security efforts and activities during the 2004 election. Our research on recommended security practices shows that effective system security management involves having, among other things, (1) defined policies governing such system controls as authorized functions and access and documented procedures for secure normal operations and incident management; (2) documented plans for implementing policies and procedures; (3) clearly assigned roles and responsibilities for system security; and (4) verified use of technical and procedural controls designed to reduce the risk of disruption, destruction, or unauthorized modification of systems and their information. Jurisdictions' efforts in each of these areas for the November 2004 general election are discussed here.

Policies and procedures. Many jurisdictions reported having written policies and procedures for certain aspects of security related to their voting systems, but others did not. Written security policies were more prevalent among large jurisdictions (an estimated 65 percent) than small jurisdictions (an estimated 41 percent). An estimated one-fifth of jurisdictions reported that they did not have written policies and procedures in place for transporting ballots or electronic memory, storing ballots, or electronic transmission of voted ballots to ensure ballot security. In

addition, some jurisdictions that we visited had published detailed voting system security policies and procedures that included such topics as network security policies for election tabulation, procedures for securing and protecting election equipment and software, testing voting equipment to ensure accurate recording of votes, and disaster recovery plans, while others omitted these topics.[19] Some jurisdictions also took additional steps to ensure that election workers had access to, and were trained in, the contents of the policies and procedures for securing ballots and voting equipment.

Implementation plans. Election officials in only 8 of the 28 jurisdictions that we visited told us that they had written plans for implementing security aspects of their voting systems and processes. Moreover, the contents of plans we obtained from local jurisdictions varied widely. One of the jurisdiction's security plans covered most aspects of the voting process, from ballot preparation through recount, while another plan was limited to the security of its vote-tallying system in a stand-alone environment. Of the 5 plans we reviewed, 2 covered almost all of the 8 security topics in our review that included risk assessment, physical controls, awareness training, and incident response, while the others covered just one or two topics.

Roles and responsibilities. In addition, security management roles and responsibilities for the 2004 general election were not consistently assigned.[20] According to survey responses, security responsibilities fell primarily to local election officials (estimated at 67 percent) for the 2004 general election, although state officials (estimated at 14 percent) and other entities (e.g., independent consultants and vendors, estimated at 24 percent) were also assigned these responsibilities. Local officials were typically

[19]To obtain a more detailed understanding of the stages of the election process, challenges associated with it in local jurisdictions, and how local election officials address those challenges, we visited and interviewed officials in a nonprobability sample of 28 local election jurisdictions in 14 states nationwide. For more details about these visits, see appendix V in GAO-06-450.

[20]From our local jurisdiction survey, we estimate that 90 percent of all jurisdictions (excluding those that used only hand-counted paper ballots on Election Day) specifically assigned responsibility for voting system security. Jurisdictions that used only hand-counted paper ballots on Election Day were excluded from this survey question.

responsible for implementing security controls, while state officials were usually involved with developing security policy and guidance and monitoring local jurisdictions' implementation of security. Some jurisdictions reported that other entities performed tasks such as securing voting equipment during transport or storage and training election personnel for security awareness. Similarly, 26 states reported that security monitoring and evaluation was performed by two or more entities. In 22 states and the District of Columbia, responsibility for security monitoring and evaluation was shared between the state and local election officials. States also reported cases where other entities (e.g., independent consultants or vendors) were involved in monitoring and evaluating controls. The entities that were assigned tasks and responsibilities at the local jurisdictions we visited are described in table 1.

Table 1: Voting System Security Tasks and Responsibilities for the 2004 General Election Reported by Election Officials in Local Jurisdictions Visited by GAO

Examples of voting system security tasks identified by local officials	Performing entity		
	Local officials	State	Other entities
Secure ballot programming	X		
Sealing of voted ballots	X		
Secure storage of voting equipment	X		X (e.g., schools)
Video surveillance of stored equipment or ballots	X		
Access control to stored election materials	X		
Protection of voting equipment and materials during transport	X		X (e.g., law enforcement officials)
Inventory management of voting equipment and ballots	X		
Monitoring vote tallying systems for unauthorized connections	X		
Impoundment of election materials after elections	X		
Monitoring and testing of equipment accuracy before, during, and after elections	X	X	X
Security awareness training for election personnel	X	X	X
Certification of voting equipment	X	X	
Development of security policies and guidance for jurisdictions	X	X	
Monitoring implementation of security policies by jurisdictions	X	X	

Source: GAO analysis of documents provided by local jurisdictions we visited.

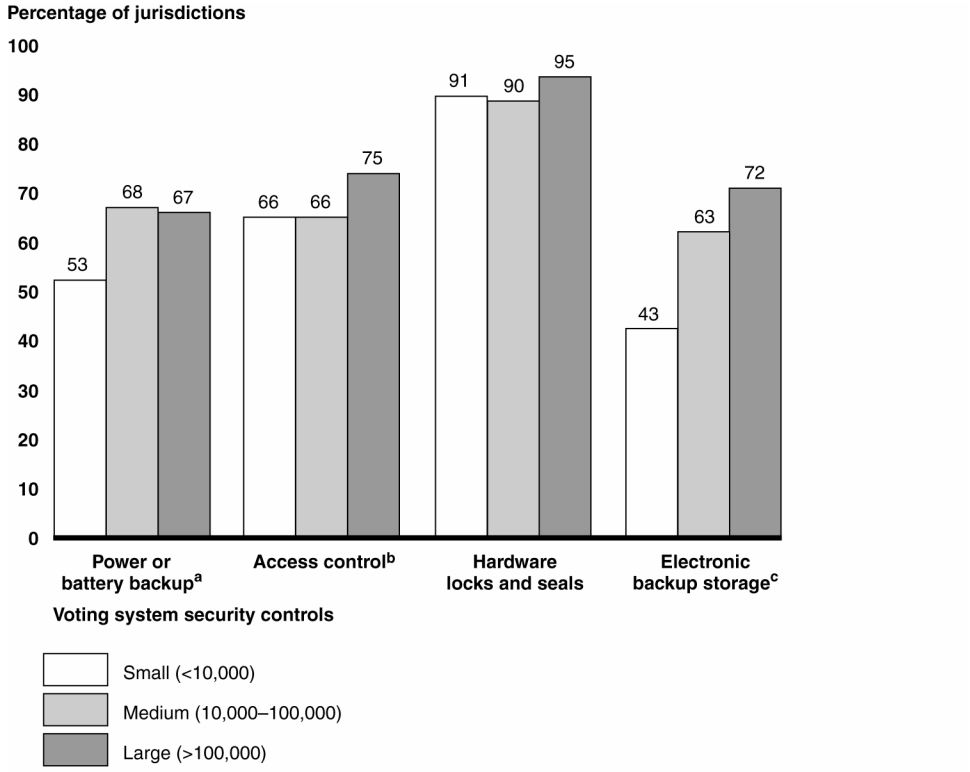
Use of security controls. For the November 2004 general election, jurisdictions' operation of voting systems employed varying uses of certain security controls.[21] Based on survey responses, we estimated that 59 percent of jurisdictions used power or battery backup, 67 percent used system access controls, 91 percent used hardware locks and seals, and 52 percent used backup electronic storage for votes.[22] We further estimated that 95 percent of jurisdictions used at least one of these controls, and we estimated hardware locks and seals were the controls most consistently used for electronic voting systems.[23] Furthermore, we estimated that a lower percentage of small jurisdictions used power or battery backup and electronic backup storage of votes for their voting systems than large or medium jurisdictions, and these differences are statistically significant in most cases. Figure 6 presents the use of various security controls by jurisdiction size.

[21]Common security controls included (1) identification names and passwords to control access to voting equipment and software, (2) redundant storage media for recovery in the event of power or equipment failure, (3) encryption to ensure privacy of votes and confidentiality of election results, (4) audit trails to document the integrity of the voting process, and (5) hardware locks and seals to prevent unauthorized access to voting equipment components.

[22]Jurisdictions that used only hand-counted paper ballots on Election Day were excluded from this survey question.

[23]We were unable to reliably estimate percentages for jurisdictions where predominant voting methods were central count punch cards or precinct count punch cards voting methods for all but one of these security controls. We estimate that 95 percent of jurisdictions where the predominant voting method was central count punch cards used hardware locks and seals.

Figure 6: Estimated Use of Security Controls by Local Jurisdictions in the 2004 General Election, by Jurisdiction Size



Source: GAO 2005 survey of local election jurisdictions.

Note: More than one group may have been identified with security responsibilities.
[a]The difference between small jurisdictions and medium jurisdictions is statistically significant. The 95 percent confidence interval for small jurisdictions is plus or minus 8 percentage points.
[b]The 95 percent confidence interval for small jurisdictions is plus or minus 8 percentage points.
[c]The differences between small jurisdictions and both medium and large jurisdictions are statistically significant. The 95 percent confidence interval for small jurisdictions is plus or minus 8 percentage points.

Among the jurisdictions that we visited, election officials reported that various security measures were in use during the 2004 general election to safeguard voting equipment, ballots, and votes before, during, and after the election. However, the measures were not uniformly reported by officials in these jurisdictions, and officials in

most jurisdictions reported that they did not have a security plan to govern the scope, nature, and implementation of these measures or other aspects of their security program. The security controls most frequently cited by officials for the jurisdictions that we visited were locked storage of voting equipment and ballots and monitoring of voting equipment. Other security measures mentioned during our visits included testing voting equipment before, during, or after the election to ensure that the equipment was accurately tallying votes; planning and conducting training on security issues and procedures for elections personnel; and video surveillance of stored ballots and voting equipment. Table 2 summarizes the types and frequency of security measures reported by election officials in the jurisdictions we visited.

Table 2: Security Controls Reportedly Used in the 2004 General Election by Election Officials in Jurisdictions Visited by GAO

Reported security control	Number of jurisdictions
Locked/sealed storage of voting equipment and ballots[a]	25
Monitoring of voting equipment[a]	14
Encrypted ballots or election results[a]	10
Security plans[a]	8
Testing of voting equipment[a]	7
Control of voting machine memory cards by precinct personnel during elections[a]	6
Video surveillance for voting equipment or ballots	5
Security training	4

Source: GAO analysis of interviews from local jurisdictions we visited.

[a]One or more jurisdictions we visited indicated this security control was not applicable because of the voting method used.

Voting systems that can be remotely accessed introduce additional security challenges. Based on survey responses, we estimated that a small percentage of local jurisdictions (10 percent) provided remote access to their voting systems for one or more categories of personnel—local election officials, state election officials, vendors, or other parties.[24] Some of the jurisdictions that provided this access described a variety of protections to mitigate the risk of

[24]Jurisdictions that used only hand-counted paper ballots on Election Day were excluded from this survey question.

unauthorized remote access, including locally controlled passwords, passwords that change for each access, and local control of communications connections. However, the percentage of jurisdictions with remote access may actually be higher because 7 to 8 percent of jurisdictions did not know if remote access was available for their systems.

Some Types of Testing Were Not Commonly Performed

To ensure that voting systems perform as intended, the systems must be effectively tested. Voting system test and evaluation can be grouped into various types, or stages: certification testing (national level), certification testing (state level), acceptance testing, readiness testing, parallel testing, and postelection voting system audits. Each of these tests has a specific purpose and is conducted at the national, state, or local level at a particular time in the election cycle. Table 3 summarizes these types of tests.

Table 3: Types of Testing and Evaluation for Voting Systems, with Common Time Frames and Responsibilities

Test type	Purpose	When conducted	Responsibility
Certification (national)[a]	To verify compliance of voting equipment with federal standards	Prior to (or as a condition of) system acceptance	Federal authorities and independent laboratories[b]
Certification (state)	To validate compliance of voting equipment with state-specific requirements	Before election	State election authorities
Acceptance	To verify that voting equipment delivered by a vendor meets state or local requirements	Before election	State or local election authorities
Readiness (logic and accuracy)	To verify that voting equipment is functioning properly, usually by confirming that predictable outputs are produced from pre-defined inputs[c]	Before election	Local election authorities
Parallel	To verify accurate performance of voting equipment through random selection and systematic evaluation of operational equipment	During election	State or local election authorities
Audit	To review and reconcile election records to confirm correct conduct of an election or uncover evidence of problems with voting equipment or election processes	After election	State or local election authorities

Source: GAO analysis based on GAO-02-3 and GAO-05-956.

[a]With the enactment of HAVA in 2002, responsibility for overseeing national testing of voting systems and certifying those that met federal standards was assigned to the EAC in HAVA § 231(a)(1) (codified at 42 U.S.C. § 15371(a)(1)). The EAC assumed this responsibility in August 2005, when it was transferred from the National Association of State Election Directors, where national testing against federal standards was called "qualification testing".
[b]Refers to the U.S. Election Assistance Commission and testing laboratories accredited by them as provided for in HAVA § 231 (codified at 42 U.S.C. § 15371).
[c]Readiness testing that is conducted to confirm the proper functioning of election equipment on Election Day just before the polls open is sometimes called verification testing.

For the November 2004 general election, voting system testing was conducted for almost all voting systems, but the types and content of the testing performed varied considerably. According to survey responses, most states and local jurisdictions employed national and state certification testing and readiness testing to some extent, but the criteria used in this testing were highly dependent on the state or jurisdiction. Also, many, but not all, states and jurisdictions conducted acceptance testing of both newly acquired systems and those undergoing changes or upgrades. In contrast, relatively few

states and jurisdictions conducted parallel testing during elections or audits of voting systems following elections. State and local responses to our surveys are summarized here relative to each type of testing.

National certification. Most states continued to require that voting systems be nationally tested and certified. For voting systems being used for the first time in the 2004 general election, national certification testing was almost always uniformly required. In particular, 26 of 27 states using DRE for the first time in this election, as well as the District of Columbia, required their systems to be nationally certified, while 9 of the 10 states using punch card equipment for the first time and 30 of 35 states and the District of Columbia using optical scan equipment for the first time, reported such requirements. However, for the 2004 general election, we estimated that 68 percent of jurisdictions did not know whether their respective systems were nationally certified. This uncertainty surrounding the certification status of a specific version of voting system at the local level underscores our concern that even though voting system software may have been qualified and certified at the national or state levels, software changes and upgrades performed at the local level may not be.

State certification. For the November 2004 general election, 42 states and the District of Columbia reported that they required state certification of voting systems. Seven of these states purchased voting systems at the state level for local jurisdictions. Officials for the remaining states and the District of Columbia reported that responsibility for purchasing a state-certified voting system rested with the local jurisdiction. While state certification requirements often included national testing as well as confirmation of functionality for particular ballot conditions, some states also required additional features such as construction quality, transportation safety, and documentation. Among the remaining 8 states that did not require state certification, officials described other mechanisms to address the compliance of voting equipment with state-specific requirements, such as a state approval process or acceptance of voting equipment based on federal certification.

For the 2006 general election, 44 states reported that they would have requirements for certification of voting systems, 2 more states

than for the 2004 general election. Of the 44, all but 1 expected to conduct the certification themselves; the remaining state reported that it would rely on results from a national independent testing authority to make its certification decision. In addition, 18 of the 43 states planned to involve a national testing laboratory in their certification process.

Acceptance testing. With regard to acceptance testing of new voting systems, 26 states and the District of Columbia reported that responsibility for such testing was assigned to either the state or local level for the 2004 general election. Specifically, 8 states and the District of Columbia reported that they had responsibility for performing acceptance testing, 15 states required local jurisdictions to perform such testing, and 3 states reported that requirements for acceptance testing existed at both the state and local levels. Twenty-two states either did not require such testing or did not believe that such testing was applicable to them. (Two states did not know what their acceptance testing requirements were for the 2004 election.)

In addition, more states required that acceptance testing be performed for changes and upgrades to existing systems than they did for new systems—30 states in all and the District of Columbia. Similarly, election officials at a majority of the local jurisdictions that we visited told us that they conducted some type of acceptance testing for newly acquired voting equipment, although they described a variety of approaches to performing acceptance testing. For example, the data used for testing could be vendor-supplied, developed by election officials, or both, and could include system initialization, logic and accuracy, and tamper resistance. Other steps, such as diagnostic tests, physical inspection of hardware, and software configuration checks, were also mentioned as testing activities by local election officials. Further, election officials from 3 jurisdictions that we visited said that vendors were heavily involved in designing and executing the acceptance tests, while officials from another jurisdiction that we visited said that vendors contributed to a portion of their testing. In 2 jurisdictions, officials said that acceptance tests were conducted at a university center for elections systems.

Readiness testing. Almost all states (49) and the District of Columbia reported that they performed readiness testing of voting

systems at the state level, the local level, or both (one state did not require readiness testing). Most states (37) required local jurisdictions to perform readiness testing. However, 7 states reported that they performed their own readiness testing for the 2004 general election in addition to local testing. Five states and the District of Columbia reported that they had no requirements for local jurisdictions to perform readiness testing but conducted this testing themselves.

State laws or regulations in effect for the 2004 election typically had specific requirements for when readiness testing should be conducted and who was responsible for testing, sometimes including public demonstrations of voting system operations. We found that most jurisdictions conducted readiness testing, also known as logic and accuracy testing, for both the 2000 and 2004 general elections. Election officials in all of the local jurisdictions we visited following the 2004 election reported that they conducted readiness testing on their voting equipment using one or more approaches, such as diagnostic tests, integration tests, mock elections, and sets of test votes, or a combination of approaches.

Security testing. Security testing was reportedly performed by 17 states and the District of Columbia for the voting systems used in the 2004 general election, and 7 other states reported that they required local jurisdictions to conduct such testing. The remaining 22 states said that they did not conduct or require system security testing. (Three states reported that security testing was not applicable for their voting systems.) Moreover, we estimated that at least 19 percent of local jurisdictions nationwide (excluding jurisdictions that reported that they used paper ballots) did not conduct security testing for the systems they used in the November 2004 election. Although jurisdiction size was not a factor in whether security testing was performed, the percentage of jurisdictions performing security testing was notably higher when the predominant voting method was DRE (63 percent[25]) and lower for

[25]The 95 percent confidence interval for DRE is plus14 or minus15 percentage points.

jurisdictions where the predominant method was precinct count optical scan (45 percent).[26]

Parallel testing. Parallel testing was not widely performed by local jurisdictions in the 2004 general election, although 7 states reported that they performed parallel testing of voting systems on Election Day, and another 6 states reported that this testing was required by local jurisdictions.[27] We estimated that 2 percent of jurisdictions using electronic systems for at least some of their voting conducted parallel testing for the 2004 general election.[28] Large and medium jurisdictions primarily performed this type of testing (7 percent and 4 percent of jurisdictions, respectively). The percentage of small jurisdictions performing this type of testing was negligible (0 percent). Election officials in 2 of the 28 jurisdictions that we visited told us that they performed parallel testing either at the state level or at the local jurisdiction. In both cases, the tests were conducted on voting equipment for which security concerns had been raised in another state's voting equipment test report. Local officials who told us that parallel testing was not performed on their voting systems attributed this to the absence of parallel testing requirements, a lack of sufficient voting equipment to perform these tests, or the view that parallel testing was unnecessary because of the stand-alone operation of their systems.

Post-election audits. Less than one-half of the states (22) and the District of Columbia reported that they performed postelection voting system audits for the 2004 general election. Specifically, 4 states and the District of Columbia reported that they conducted postelection audits of voting systems, 16 states required that audits of voting systems be conducted by local jurisdictions, and 2 states reported that audits of voting systems were performed at both the state and local levels. Moreover, state laws or regulations in effect

[26]The 95 percent confidence interval for precinct count optical scan is plus or minus 9 percentage points. The difference between the percentages of jurisdictions performing security testing on DRE and central count optical scan was not statistically significant.

[27]Both EAC's *Best Practices Tool Kit* and the 2005 *Voluntary Voting System Guidelines* recommend development of parallel testing procedures for all types of automated voting equipment.

[28]We estimated that 91 percent of jurisdictions considered parallel testing to be not applicable.

for the 2004 general election varied in when and how these audits were to be conducted.

We estimated that 43 percent of jurisdictions that used voting systems for at least some of their voting conducted postelection voting system audits. This practice was much more prevalent at large and medium jurisdictions (62 percent and 55 percent, respectively) than small jurisdictions (34 percent).[29] We further estimated that these voting system audits were conducted more frequently in jurisdictions with central count optical scan voting methods (54 percent) than they were in jurisdictions with precinct count optical scan voting methods (35 percent).

Jurisdictions Did Not Consistently Monitor Voting System Performance

It is important that performance be measured during system operation. As we reported in 2001 and 2006, measuring how well voting systems perform during a given election allows local officials to better position themselves for ensuring that elections are conducted properly. Such measurement also provides the basis for knowing where performance needs, requirements, and expectations are not being met so that timely corrective action can be taken to ensure the security and reliability of the voting system. Jurisdictions without supporting measures for security and reliability may lack sufficient insight into their system operations.

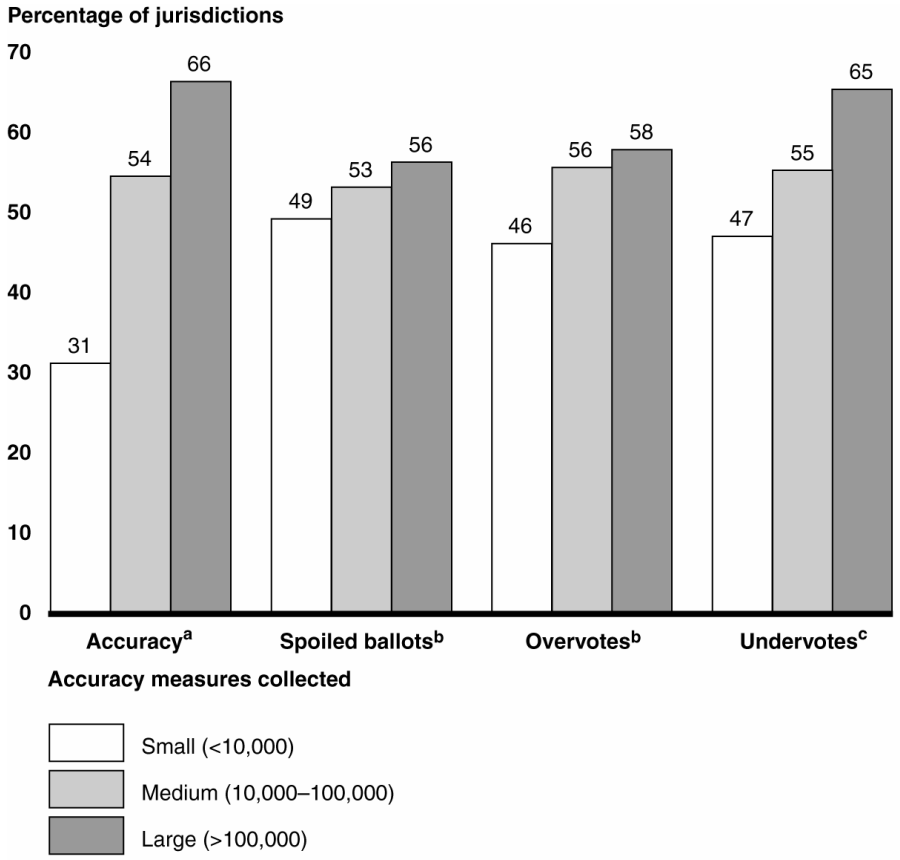
Overall, responses to our local jurisdiction survey show that large jurisdictions were most likely to record voting system performance and small jurisdictions were least likely. We estimated that 42 percent of jurisdictions overall monitored the accuracy of voting equipment in the 2004 general election. Other measures recorded were spoiled ballots (estimated at 50 percent of jurisdictions), undervotes (50 percent of jurisdictions),[30] and overvotes (49 percent of jurisdictions). During our visits to local jurisdictions, election officials in several jurisdictions told us that measuring overvotes was not a relevant performance indicator for jurisdictions using

[29]The 95 percent confidence interval for large jurisdictions is plus or minus 8 percentage points, and for small jurisdictions it is plus or minus 7 percentage points.

[30]An estimated 25 percent of respondents selected "not applicable" to the question on spoiled/ruined ballots in their survey response.

DREs because they do not permit overvoting, and that undervotes were not a meaningful metric because most voters focused on a limited range of issues or candidates and thus frequently chose not to vote on all contests. Figure 7 shows the percentages of small, medium and large jurisdictions that collected information on various measures of accuracy.

Figure 7: Estimated Percentages of Jurisdictions that Collected Information on Voting Accuracy for the 2004 General Election, by Jurisdiction Size



Source: GAO 2005 survey of local election jurisdictions.

[a]The differences between small jurisdictions and both medium and large jurisdictions are statistically significant.

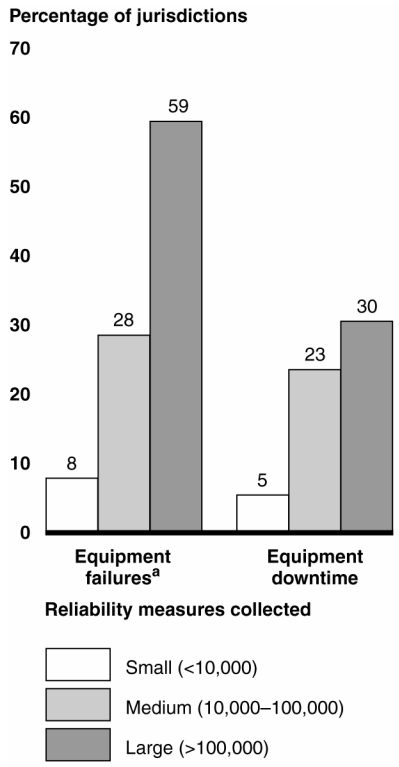
[b]The 95 percent confidence interval for small jurisdictions in these categories is plus or minus 6 percentage points.

[c]The difference between small jurisdictions and large jurisdictions is statistically significant. The 95 percent confidence interval for small jurisdictions is plus or minus 6 percentage points.

We estimated that 15 percent of jurisdictions measured voting system failure rates and 11 percent measured system downtime.[31] A higher percentage of large and medium jurisdictions collected these performance data than small jurisdictions. Collection of these data was also related to the predominant voting method used by a jurisdiction, with jurisdictions that predominantly used DREs more likely to collect system data than those that used precinct count or central count optical scan voting methods (an estimated 45 percent of jurisdictions versus 23 percent or 10 percent, respectively). Figure 8 shows the percentages of small, medium, and large jurisdictions that collected information on voting equipment failures and downtime. Figure 9 shows the percentages by predominant voting method of all jurisdictions that collected data on equipment failures.

[31]An estimated 66 percent of respondents selected the response "not applicable" for the survey questions on measurement of pieces of equipment that failed and equipment downtime.

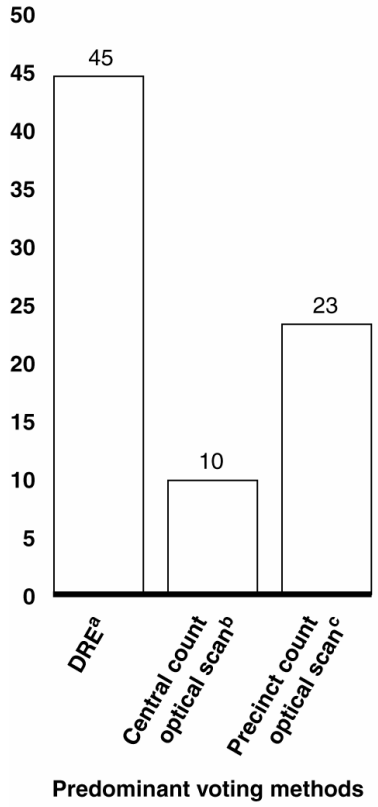
Figure 8: Estimated Percentages of Jurisdictions that Collected Information on Voting Equipment Reliability for the 2004 General Election, by Jurisdiction Size



Source: GAO 2005 survey of local election jurisdictions.

[a]The differences between all categories of jurisdiction size are statistically significant.

Figure 9: Estimated Percentages of Jurisdictions that Collected Information on Voting Equipment Failures for the 2004 General Election, by Predominant Voting Method



Source: GAO 2005 survey of local election jurisdictions.

Note: The differences between DRE and both central count and precinct count optical scan voting methods are statistically significant.
[a]The 95 percent confidence interval for DRE is plus or minus 13 percentage points.
[b]The 95 percent confidence interval for central count optical scan percentages is plus 7 or minus 5 percentage points.
[c]The 95 percent confidence interval for precinct count optical scan percentages is plus 8 or minus 7 percentage points.

Further, an estimated 55 percent of all jurisdictions kept a written record of issues and problems that occurred on Election Day, which could be a potential source of performance data. Large jurisdictions were more likely to keep a written record of issues or problems that occurred on Election Day. Specifically, we estimated that 79 percent of large jurisdictions kept such records, compared with 59 percent

of medium jurisdictions and 52 percent of small jurisdictions.[32] The responsibilities for monitoring or reporting voting system performance most often rested with local jurisdictions. We estimated that 83 percent of local jurisdictions had local officials responsible for performance monitoring or reporting, while states or other organizations (such as independent consultants or vendors) held such responsibilities in 11 percent and 13 percent of jurisdictions, respectively.

Addressing Voting System Challenges Requires the Combined Efforts of All Levels of Government

The challenges in ensuring that voting systems perform securely and reliably are not unlike those faced by any technology user—application of well-defined standards for system capabilities and performance; effective integration of the people, processes, and technology throughout the voting system life cycle; rigorous and disciplined performance of security and testing activities; objective measurement to determine whether the systems are performing as intended; and analytical and economically justified bases for making informed decisions about voting system investment options. These challenges are complicated by other conditions common to both the national elections community and other information technology environments: the distribution of responsibilities among various organizations, technology changes, funding opportunities and constraints, changing requirements and standards, and public attention. Although responsibility for voting system performance falls largely on local governmental units, state and federal governments have important roles to play as well. Therefore, all levels of government need to work together to address these challenges, under the leadership of the EAC.

To assist the EAC in executing its leadership role, we previously made recommendations to the commission aimed at better planning its ongoing and future activities relative to, for example, system standards and information sharing. While the EAC agreed with the

[32]The differences between large jurisdictions and both medium and small jurisdictions are statistically significant.

recommendations, it told us that its ability to effectively execute its role is resource constrained.

Establishing and Applying Current and Comprehensive Standards

The extent to which states and local jurisdictions adopt and consistently apply up-to-date voting system standards directly affects the security and reliability of voting systems during elections. For the 2006 general election, a substantial proportion of states and jurisdictions had yet to adopt the most current federal voting system standards or related performance measures, meaning that the systems they employ may not perform as securely and reliably as desired. Beyond this, decisions by states and local jurisdictions to apply these latest standards for the 2008 election present additional challenges such as (1) whether the systems can be tested and certified in time for the election and (2) adopting standards that are now undergoing revision rather than continued use of earlier standards or later adoption of even newer standards.

EAC plays an important role in ensuring the timely testing and certification of voting systems against the latest standards and in informing state and local decisions on whether to adopt these standards for the 2008 election. Accordingly, we have recommended that EAC define tasks and time frames for achieving the full operational capability of the national voting system certification program. These management elements would need to take into account estimating testing capacity and expected volume for the testing laboratory accreditation program, establishing protocols and time frames for reviewing certification packages, and setting norms for timely consideration and decision making regarding system certifications. Sharing this information with state and local election officials would help them to plan for system upgrades, testing, and state certification to meet their upcoming election cycles.

States and local jurisdictions must also consider the timely adoption of standards in light of the additional work that is currently under way and planned to address known weaknesses in the national standards. For example, in addition to establishing minimum functional and performance requirements for voting systems, standards can also be used to govern integration of election systems, such as the accuracy, reliability, privacy, and security of

components and interfaces. Accordingly, we have recommended that the EAC collaborate with NIST and the Technical Guidelines Development Committee to define the specific tasks, measurable outcomes, milestones, and resource needs required to improve the voting system standards. Identifying the incremental improvements to standards for several future election cycles and coordinating these with states and local jurisdictions would help those officials plan for these cycles and prepare the public for expected changes in voting technologies, security and reliability features, and compensating controls.

Ensuring that Necessary Security, Testing, and Operational Activities Are Effectively Performed

Maximizing the performance of the voting systems that jurisdictions currently have and those they plan to use in the next general election means taking proactive steps between now and November 2008 to ensure that these systems perform as intended. These steps include activities aimed at securing, testing, and preparing these systems for operation. Although the vast majority of jurisdictions performed security, testing, and operational activities in one form or another for the 2004 general election, the extent and nature of these activities varied among jurisdictions and depended on the availability of resources (financial and human capital) committed to them. The challenge facing all voting jurisdictions will be to ensure that these activities are fully and properly performed, particularly in light of the security and reliability concerns that have been reported with electronic voting systems.

Security, testing, and operational activities are to a large degree responsive to—and limited by—formal state and local directives. For 2004, election officials for some states identified various state and local directives for managing the security and reliability of their voting systems, including security plans, security testing, system acceptance testing, and voting equipment auditing. When appropriately defined and implemented, such directives can promote the effective execution of security and testing practices across all phases of the election process. As voting technologies and requirements evolve, states and local jurisdictions face the challenge

of adapting and implementing the directives to meet the needs of their specific election environments.

Managing the People, Processes, and Technology as Components of the Overall Process

As previously stated, jurisdictions need to manage the triad of people, processes, and technology as interrelated and interdependent parts of the total voting process. Given the amount of time that remains between now and the November 2008 elections, jurisdictions' voting system performance is more likely to be influenced by improvements in poll worker system operation training, voter education about system use, and vote casting and counting procedures than by changes to the physical systems. The challenge for voting jurisdictions is thus to ensure that these people and process issues are dealt with effectively.

In this regard, the election management decisions and practices of states and local jurisdictions can benefit from the experiences and results of those with comparable election environments. In 2004 and again in 2006, EAC compiled such information into guidance documents for widespread use by election officials. However, as the election environment and voting systems continue to evolve, additional lessons and topics will undoubtedly surface. Accordingly, we have recommended that the EAC establish a process and schedule for periodically compiling and disseminating recommended practices for security and reliability across the system life cycle and that the practices be informed by information it collects on the problems and vulnerabilities of these systems. Incorporating the feedback obtained through actual voting system development, acquisition, preparation, and operations into practical guidance will allow the election community to be more robust and efficient.

Gathering and Using Reliable System Performance Measures and Data and Making Informed Investment Decisions

Reliable measures and objective data are needed for jurisdictions to know whether the technology they use is meeting the needs of the user communities (both the voters and the officials who administer the elections). While the vast majority of jurisdictions reported that they were satisfied with the performance of their respective

technologies in the November 2004 elections, this satisfaction was based mostly on the subjective impressions of election officials rather than on objective data that measured voting system performance. Although these impressions should not be discounted, informed decision making on voting system operations and technology investment requires more objective data. The immediate challenge for jurisdictions is to define measures and begin collecting data so that they can definitely know how their systems are performing.

States and local jurisdictions can benefit from sharing performance data on voting systems, including information on problems and vulnerabilities. However, the diffused and decentralized nature of our election system impedes timely and accurate collection and dissemination of this type of information for particular voting system models. Accordingly, we have recommended that the EAC develop a process and associated time frames for sharing information on voting system problems and vulnerabilities across the election community. The national voting system certification process established in January 2007 provides a mechanism for election officials to report problems and vulnerabilities with their systems to the EAC. Not yet defined are the mechanisms to collect and disseminate information on problems and vulnerabilities that are identified by voting system vendors and independent groups outside of the national certification process.

In addition, foreseeable changes in technology require jurisdictions to determine whether a particular technology will provide benefits that are commensurate with life cycle costs (acquisition as well as operation and maintenance) and to assess whether these collective costs are affordable and sustainable. Thus, the long-term challenge for jurisdictions is to view and treat voting systems as capital investments and to manage them as such, including basing decisions on technology investments on clearly defined requirements and reliable analyses of quantitative and qualitative return on investment.

In closing, I would like to say again that electronic voting systems are an undeniably critical link in the overall election chain. While

this link alone cannot make an election, it can break one. The problems that some jurisdictions have experienced and the serious concerns that have surfaced highlight the potential for continuing difficulties in upcoming national elections if these challenges are not effectively addressed. The EAC plays a vital role related to ensuring that election officials and voters are educated and well informed about the proper implementation and use of electronic voting systems and ensuring that jurisdictions take the appropriate steps—related to people, process, and technology—that are needed regarding security, testing, and operations. More strategically, the EAC needs to move swiftly to strengthen the voting system standards and the testing associated with enforcing them. However, the EAC alone cannot ensure that electronic voting system challenges are effectively addressed. State and local governments must also do their parts. Moreover, critical to the commission's ability to do its part will be the adequacy of resources at its disposal and the degree of cooperation it receives from entities at all levels of government.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other Members of the Subcommittee may have at this time.

Contact and Acknowledgments

For further information, please contact Randolph C. Hite at (202) 512-3439 or by e-mail at hiter@gao.gov. Other key contributors to this testimony were Nancy Glover, Paula Moore, Sushmita Srikanth and Kim Zelonis.

(310645)