United States Government Accountability Office

GAO

Report to Congressional Requesters

September 2005

ELECTIONS

Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed

GAO-05-956

September 2005

ELECTIONS

Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed

GAO Highlights

Highlights of GAO-05-956, a report to congressional requesters

Why GAO Did This Study

The Help America Vote Act of 2002 established the Election Assistance Commission (EAC) to help improve state and local administration of federal elections and authorized funding for state and local governments to expand their use of electronic voting systems. EAC began operations in January 2004. However, reported problems with electronic voting systems have led to questions about the security and reliability of these systems. GAO was requested to (1) determine the significant security and reliability concerns identified about electronic voting systems, (2) identify recommended practices relevant to ensuring the security and reliability of these systems, and (3) describe actions taken or planned to improve their security and reliability.

What GAO Recommends

To help ensure the security and reliability of electronic voting systems, GAO is recommending that EAC define specific tasks, processes, and time frames for improving the national voting systems standards, testing capabilities, and management support available to state and local election officials. In commenting on a draft of this report, EAC agreed with the recommendations and stated that the commission has initiatives under way or planned in these areas. The commission also sought additional clarification and context on reported problems.

www.gao.gov/cgi-bin/getrpt?GAO-05-956.

To view the full product, including the scope and methodology, click on the link above. For more information, contact David Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

While electronic voting systems hold promise for improving the election process, numerous entities have raised concerns about their security and reliability, citing instances of weak security controls, system design flaws, inadequate system version control, inadequate security testing, incorrect system configuration, poor security management, and vague or incomplete voting system standards (see below for examples). It is important to note that many of these concerns were based on specific system makes and models or a specific jurisdiction's election, and there is no consensus among election officials and other experts on their pervasiveness. Nevertheless, some have caused problems in elections and therefore merit attention.

Federal organizations and nongovernmental groups have issued both election-specific recommended practices for improving the voting process and more general guidance intended to help organizations manage information systems' security and reliability. These recommended practices and guidelines (applicable throughout the voting system life cycle) include having vendors build security controls and audit trails into their systems during development, and having election officials specify security requirements when acquiring systems. Other suggested practices include testing and certifying systems against national voting system standards.

The federal government has begun efforts intended to improve life cycle management of electronic voting systems and thereby improve their security and reliability. Specifically, EAC has led efforts to (1) draft changes to existing federal voluntary standards for voting systems, including provisions addressing security and reliability; (2) develop a process for certifying voting systems; (3) establish a program to accredit independent laboratories to test electronic voting systems; and (4) develop a library and clearinghouse for information on state and local elections and systems. However, these actions are unlikely to have a significant effect in the 2006 federal election cycle because important changes to the voting standards have not yet been completed, the system certification and laboratory accreditation programs are still in development, and a system software library has not been updated or improved since the 2004 election. Further, EAC has not consistently defined specific tasks, processes, and time frames for completing these activities; as a result, it is unclear when their results will be available to assist state and local election officials.

Examples of Voting System Vulnerabilities and Problems

- Cast ballots, ballot definition files, and audit logs could be modified.
- Supervisor functions were protected with weak or easily guessed passwords.
- Systems had easily picked locks and power switches that were exposed and unprotected.
- Local jurisdictions misconfigured their electronic voting systems, leading to election day problems.
- Voting systems experienced operational failures during elections.
- Vendors installed uncertified electronic voting systems.

Source: GAO analysis of recent reports and studies.

Contents

Figures

Abbreviations

COTS	commercial off-the-shelf
DRE	Direct Recording Electronic
EAC	Election Assistance Commission
HAVA	Help America Vote Act
IT	information technology
NIST	National Institute of Standards and Technology
TGDC	Technical Guidelines Development Committee

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, D.C. 20548

September 21, 2005

Congressional Requesters

After the 2000 elections, Congress, the media, and others cited numerous instances of problems with the election process. In light of these concerns, we produced a series of reports in which we examined virtually every aspect of the election process, including challenges associated with electronic voting systems.[1] In these reports, we emphasized the contributions and necessary interactions of people, process, and technology to address these challenges. Subsequently, in October 2002, Congress passed the Help America Vote Act (HAVA), which authorized funding for local and state governments to make improvements in election administration, including upgrading antiquated voting systems. In addition, HAVA created the Election Assistance Commission (EAC) to provide support for election improvements and to administer payments to states under the act. As states have expanded their use of electronic voting systems, the media and others have reported problems with these systems that have caused some to question whether they are secure and reliable.

In view of the importance and growing role of electronic voting systems, you asked us to (1) determine the significant security and reliability concerns that have been identified about these voting systems; (2) identify recommended practices relevant to ensuring the security and reliability of such systems; and (3) describe the actions that federal agencies and other organizations have taken, or plan to take, to improve their security and reliability. To determine concerns and recommended practices, we analyzed over 80 recent and relevant reports related to the security and reliability of electronic voting systems. We focused on systems and components associated with vote casting and counting, including those that define electronic ballots, transmit voting results among election locations, and manage groups of voting machines. We assessed the various types of voting system issues reported to determine categories of concerns. We discussed the reports, concerns, and recommended practices with elections officials, citizen advocacy groups, and system security and testing experts, including members of GAO's Executive Council on Information

[1]GAO, *Elections: Perspectives on Activities and Challenges Across the Nation*, GAO-02-3 (Washington, D.C.: Oct. 15, 2001); *Elections: Status and Use of Federal Voting Equipment Standards*, GAO-02-52 (Washington, D.C.: Oct. 15, 2001); and *Elections: A Framework for Evaluating Reform Proposals*, GAO-02-90 (Washington, D.C.: Oct. 15, 2001).

Management and Technology.[2] To describe actions to improve the security and reliability of electronic voting systems, we reviewed and analyzed pertinent documentation, such as EAC's draft voluntary voting system guidelines (which are expected to replace the 2002 voting system standards), and we attended public meetings and interviewed officials from EAC, its Technical Guidelines Development Committee (TGDC), and the Department of Commerce's National Institute of Standards and Technology (NIST). We also identified activities being performed by citizen advocacy groups, academic and standards bodies, and others that are intended to improve the security and reliability of electronic voting systems, reviewed materials from these activities, and discussed them with representatives of these groups. Appendix I provides additional details on our objectives, scope, and methodology. We performed our work from January through August 2005 in the Washington, D.C., metropolitan area, in accordance with generally accepted government auditing standards.

Results in Brief

While electronic voting systems hold promise for a more accurate and efficient election process, numerous entities have raised concerns about their security and reliability, citing instances of weak security controls, system design flaws, inadequate system version control, inadequate security testing, incorrect system configuration, poor security management, and vague or incomplete voting system standards, among other issues. For example, studies found (1) some electronic voting systems did not encrypt cast ballots or system audit logs, and it was possible to alter both without being detected; (2) it was possible to alter the files that define how a ballot looks and works so that the votes for one candidate could be recorded for a different candidate; and (3) vendors installed uncertified versions of voting system software at the local level. It is important to note that many of the reported concerns were drawn from specific system makes and models or from a specific jurisdiction's election, and that there is a lack of consensus among election officials and other experts on the pervasiveness of the concerns. Nevertheless, some of these concerns were reported to have caused local problems in federal elections—resulting in the loss or miscount of votes—and therefore merit attention.

[2]GAO's Executive Council on Information Management and Technology is made up of leading executives in government, industry, and academia.

Federal organizations and nongovernmental groups have issued recommended practices and guidance for improving the election process, including electronic voting systems, as well as general practices for the security and reliability of information systems. For example, in mid-2004, EAC issued a compendium of practices recommended by election experts, including state and local election officials.[3] This compendium includes approaches for making voting processes more secure and reliable through, for example, risk analysis of the voting process, poll worker security training, and chain of custody controls for election day operations, along with practices that are specific to ensuring the security and reliability of different types of electronic voting systems. As another example, in July 2004, the California Institute of Technology and the Massachusetts Institute of Technology issued a report containing recommendations pertaining to testing equipment, retaining audit logs, and physically securing voting systems.[4] In addition to such election-specific practices, numerous recommended practices are available that can be applied to any information system. For instance, we, NIST, and others have issued guidance that emphasizes the importance of incorporating security and reliability into the life cycle of information systems through practices related to security planning and management, risk management, and procurement.[5] The recommended practices in these election-specific and information technology (IT) focused documents provide valuable guidance that, if implemented effectively, should help improve the security and reliability of voting systems.

[3]EAC, *Best Practices Tool Kit* (July 2004), http://www.eac.gov/bp/docs/BestPracticesToolKit.doc.

[4]California Institute of Technology/Massachusetts Institute of Technology (Caltech/MIT), *Immediate Steps to Avoid Lost Votes in the 2004 Presidential Elections: Recommendations for the Election Assistance Commission* (July 2004).

[5]For example, GAO, *Federal Information Systems Controls Audit Manual*, GAO/AIMD-12-19.6 (Washington, D.C.: January 1999); NIST, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, SP 800-14 (September 1996) and *Security Considerations in the Information System Development Life Cycle*, SP 800-64, Revision 1 (June 2004); and International Systems Security Engineering Association, *Systems Security Engineering Capability Maturity Model*, ISO/IEC 21827, version 3.0 (June 2003).

Since the passage of HAVA in 2002, the federal government has begun a range of actions that are expected to improve the security and reliability of electronic voting systems. Specifically, after beginning operations in January 2004, EAC has led efforts to (1) draft changes to the existing federal voluntary standards[6] for voting systems, including provisions related to security and reliability, (2) develop a process for certifying, decertifying, and recertifying voting systems, (3) establish a program to accredit the national independent testing laboratories that test electronic voting systems against the federal voluntary standards, and (4) develop a software library and clearinghouse for information on state and local elections and systems. However, these actions are unlikely to have a significant effect in the 2006 federal election cycle because the changes to the voluntary standards have not yet been completed, the system certification and laboratory accreditation programs are still in development, and the software library has not been updated or improved since the 2004 elections. Further, EAC has not defined tasks, processes, and time frames for completing these activities. As a result, it is unclear when the results will be available to assist state and local election officials. In addition to the federal government's activities, other organizations have actions under way that are intended to improve the security and reliability of electronic voting systems. These actions include developing and obtaining international acceptance for voting system standards, developing voting system software in an open source environment (i.e., not proprietary to any particular company), and cataloging and analyzing reported problems with electronic voting systems.

To improve the security and reliability of electronic voting systems, we are recommending that EAC establish tasks, processes, and time frames for improving the federal voluntary voting system standards, testing capabilities, and management support available to state and local election officials.

EAC and NIST provided written comments on a draft of this report (see apps. V and VI). EAC commissioners agreed with our recommendations and stated that actions on each are either under way or intended. NIST's director agreed with the report's conclusions. In addition to their

[6]The Federal Election Commission used the general term "voting system standards" for its 2002 publication *Voting Systems Performance and Test Standards*. Consistent with HAVA terminology, EAC refers to its revisions of these standards as *Voluntary Voting System Guidelines*. For this report, we refer to the contents of both of these documents as "standards."

comments on our recommendations, EAC commissioners expressed three concerns with our use of reports produced by others to identify issues with the security and reliability of electronic voting systems. Specifically, EAC sought (1) additional clarification on our sources, (2) context on the extent to which voting system problems are systemic, and (3) substantiation of claims in the reports issued by others. To address these concerns, we provided additional clarification of sources where applicable. Further, we note throughout our report that many issues involved specific system makes and models or circumstances in the elections of specific jurisdictions. We also note that there is a lack of consensus on the pervasiveness of the problems, due in part to a lack of comprehensive information on what system makes and models are used in jurisdictions throughout the country. Additionally, while our work focused on identifying and grouping problems and vulnerabilities identified in issued reports and studies, where appropriate and feasible, we sought additional context, clarification, and corroboration from experts, including election officials, security experts, and key reports' authors. EAC commissioners also expressed concern that we focus too much on the commission, and noted that it is one of many entities with a role in improving the security and reliability of voting systems. While we agree that EAC is one of many entities with responsibilities for improving the security and reliability of voting systems, we believe that our focus on EAC is appropriate, given its leadership role in defining voting system standards, in establishing programs both to accredit laboratories and to certify voting systems, and in acting as a clearinghouse for improvement efforts across the nation. EAC and NIST officials also provided detailed technical corrections, which we incorporated throughout the report as appropriate.

Background

All levels of government share responsibility in the U.S. election process. At the federal level, Congress has authority under the Constitution to regulate presidential and congressional elections and to enforce prohibitions against specific discriminatory practices in all federal, state, and local elections. Congress has passed legislation that addresses voter registration, absentee voting, accessibility provisions for the elderly and handicapped, and prohibitions against discriminatory practices.[7]

[7]GAO-02-3.

At the state level, individual states are responsible for the administration of both federal elections and their own elections. States regulate the election process, including, for example, the adoption of voluntary voting system guidelines, the state certification and acceptance testing of voting systems, ballot access, registration procedures, absentee voting requirements, the establishment of voting places, the provision of election day workers, and the counting and certification of the vote. In total, the U.S. election process can be seen as an assemblage of 55 distinct election systems—those of the 50 states, the District of Columbia, and the 4 U.S. territories.

Further, although election policy and procedures are legislated primarily at the state level, states typically have decentralized voting processes, so that the details of administering elections are carried out at the city or county levels, and voting is done at the local level. As we reported in 2001, local election jurisdictions number more than 10,000, and their sizes vary 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.[8]

Administering an election is a year-round process involving the following stages:

- *Voter registration.* Local election officials register eligible voters and maintain voter registration lists. This includes updating registrants' information and deleting the names of registrants who are no longer eligible to vote.

- *Absentee and early voting.* Election officials design ballots and other systems to permit eligible people to vote in person or by mail before election day. Election officials also educate voters on how to vote by these methods.

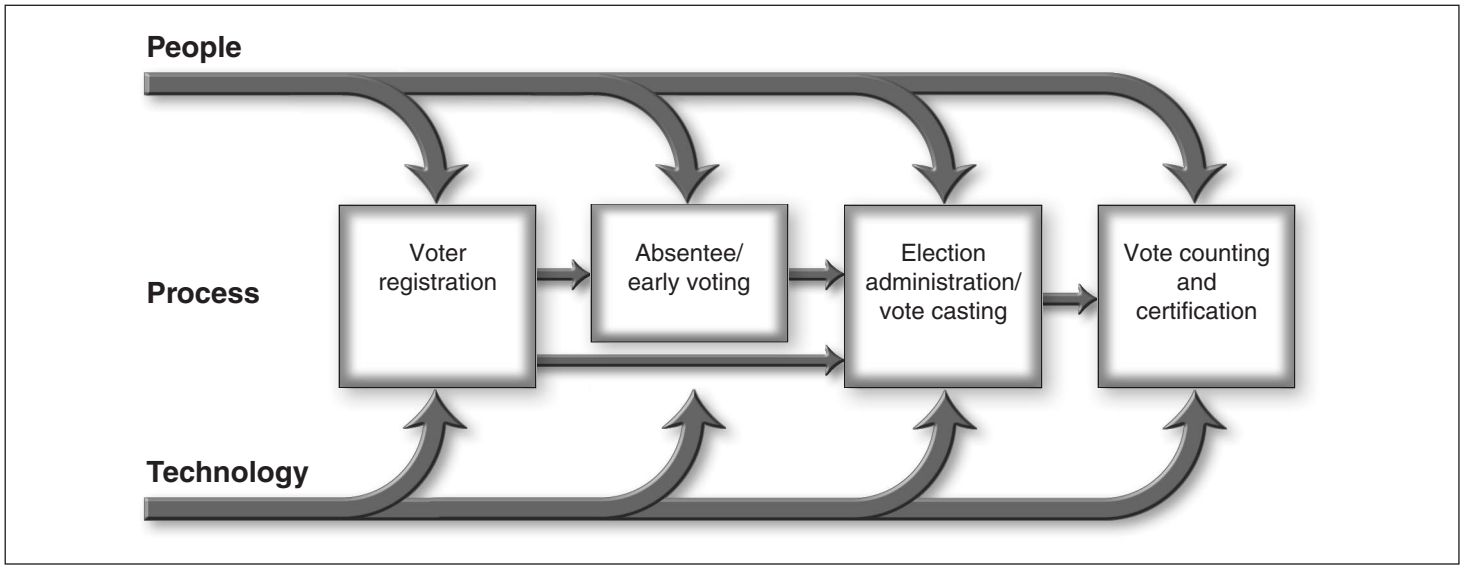
- *Election administration and vote casting.* Election officials prepare for an election by arranging for polling places, recruiting and training poll workers, designing ballots, and preparing and testing voting equipment for use in casting and tabulating votes. Election day activities include opening and closing polling places and assisting voters in casting votes.

[8]GAO-02-3.

- *Vote counting and certification.* 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 1, each stage of an election involves people, processes, and technology.

Figure 1: Stages of an Election Process



Source: GAO analysis.

Electronic Voting Systems Support Vote Casting and Counting

Electronic voting systems hold promise for improving the efficiency and accuracy of the election process by automating a manual process, providing flexibility for accommodating voters with special needs, and implementing controls to avoid errors by voters and election workers.

In the United States today, most votes are cast and counted by one of two types of electronic voting systems: optical scan systems and direct recording electronic (DRE) systems. Such systems include the hardware, software, and firmware used to define ballots, cast and count votes, report or display election results, and maintain and produce audit trail

information—as well as the documentation required to program, control, and support the equipment. A description of both technologies follows.

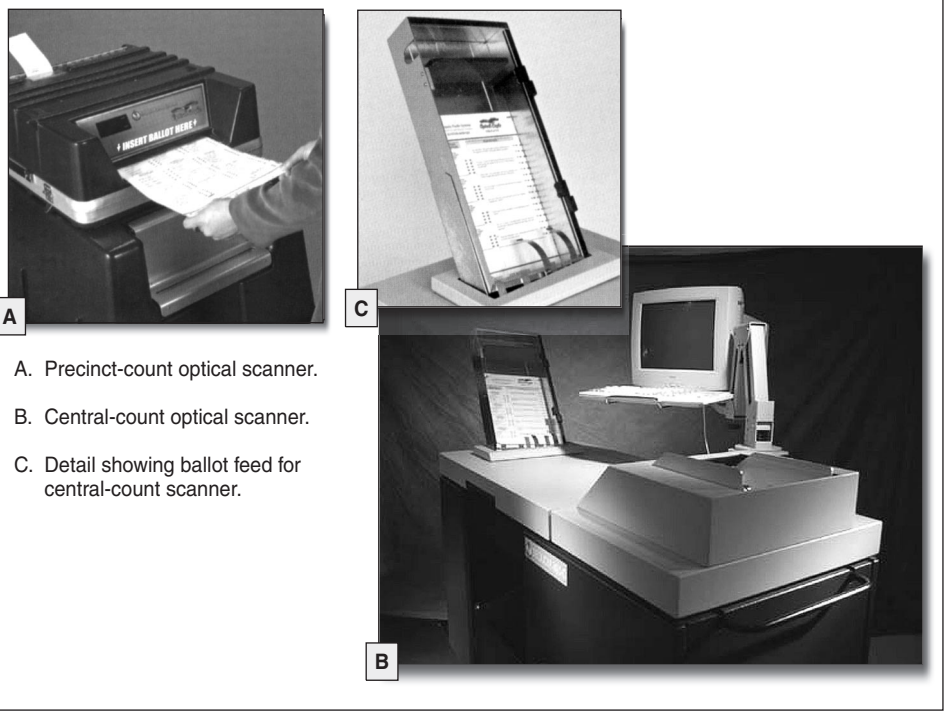
Optical Scan Systems. Optical scan voting systems use electronic technology to tabulate paper ballots. Although optical scan technology has been in use for decades for such tasks as scoring standardized tests, it was not applied to voting until the 1980s. According to Election Data Services, Inc., a firm specializing in election data statistics, about 31 percent of registered voters voted on optical scan systems in the 2000 election, and about 35 percent of registered voters voted on optical scan systems in the 2004 election.

An optical scan system is made up of computer-readable paper 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 a candidate's name or the issue. In some states, the ballot may include a space for write-ins to be entered 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—referred to as a precinct-count optical scan[9]—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 in the presence of observers.

[9]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



A. Precinct-count optical scanner.

B. Central-count optical scanner.

C. Detail showing ballot feed for central-count scanner.

Source: Equipment vendors.

Software instructs the tabulation equipment how 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 votes for two candidates for one office, for example, 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). In addition, optical scan systems often use vote-tally software to tally the vote totals from one or more vote tabulation devices.

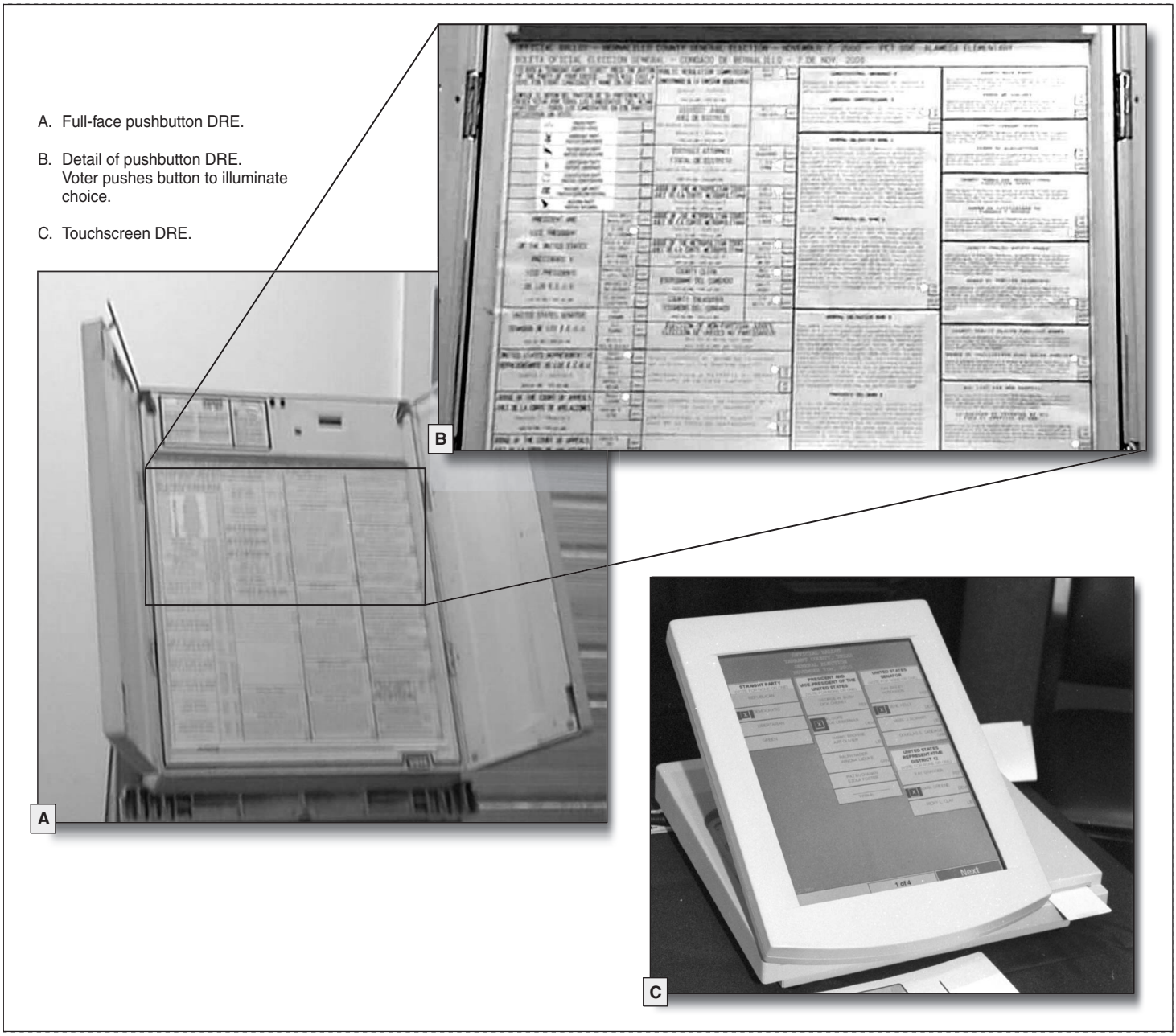
If election officials program precinct-based optical scan systems to detect and reject overvotes and undervotes, voters can fix their mistakes before leaving the polling place. However, if voters are unwilling or unable to

correct their ballots, a poll worker can manually override the program and accept the ballot, even though it has been overvoted or undervoted. If ballots are tabulated centrally, voters would not be able to correct any mistakes that may have been made.

Direct Recording Electronic (DRE) Systems. First introduced in the 1970s, DREs capture votes electronically, without the use of paper ballots. According to Election Data Services, Inc., about 12 percent of voters used this type of technology in the 2000 elections and about 29 percent of voters used this technology in the 2004 elections.

DREs come in two basic models: pushbutton or touchscreen. The pushbutton model is the older technology and is larger and heavier than the touchscreen model (see fig. 3).

Figure 3: Two Types of DRE Systems—Pushbutton and Touchscreen



Source: Local election officials and equipment vendor.

Pushbutton and touchscreen models also differ significantly in the way they present ballots to the voter. With the pushbutton model, 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, touchscreen DREs display the ballot information on an electronic display screen. For both pushbutton and touchscreen models, the ballot information is programmed onto an electronic storage medium, which is then uploaded to the machine. Both models rely on ballot definition files to tell the voting machine software how to display ballot information on the screen, interpret a voter's touches on a button or screen, and record and tally those selections as votes. Local jurisdictions can program these files before each election or outsource their programming to a vendor. For touchscreens, ballot information can be displayed in color and can incorporate pictures of the candidates. Because the ballot space on a touchscreen is much smaller than on a pushbutton machine, voters who use touchscreens must page through the ballot information.

Despite their differences, the two DRE models have some similarities, such as how the voter interacts with the voting equipment. For pushbutton models, voters press a button next to the candidate or issue, which then lights up to indicate the selection. Similarly, voters using touchscreens make their selections by touching the screen next to the candidate or issue, which is then highlighted. When voters have finished making their selections on a touchscreen or a pushbutton model, 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. Both models also 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. Further, although these systems do not use paper ballots, they 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 can be printed and used for auditing and recounts.

Some of the newer DREs use smart cards 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. These cards are generally used as a means to open polls and to authorize voter access to ballots. For instance, smart cards for some systems store program data on the election and are used to help set up the equipment; during setup, election workers verify that the card is for the proper election. Other

systems are programmed to automatically activate when the voter inserts a smart card; the card brings up the correct ballot onto the screen. In general, the interface with the voter is very similar to that of an automated teller machine.

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. The software is used to generate ballots for each precinct in the voting jurisdiction, which includes defining the ballot layout, identifying the contests in each precinct, and assigning candidates to contests. The software also is used to configure any special options, such as straight party voting and vote-for-no-more-than-N contests. In addition, for pushbutton models, the software assigns the buttons to particular candidates, and, for touchscreen models, the software defines the size and location on the screen where the voter makes the selection. Vote-tally software is often used to tally the vote totals from one or more units.

DRE systems 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.

These systems are also designed not to allow overvotes. For example, if a voter selects a second choice in a two-way race, the first choice is deselected. In addition to this standard feature, different types of systems offer a variety of options, including many aimed at voters with disabilities. In our prior work,[10] we reported that the following features were available on some models of DRE:

- *A "no-vote" option.* If allowed by the state, this option helps avoid unintentional undervotes. This provides the voter with the option to select "no vote" (or abstain) on the display screen if the voter does not want to vote on a particular contest or issue.

- *A "review" feature.* This feature requires voters to review each page of the ballot before pressing the button to cast the vote.

[10]GAO-02-3.

- *Visual enhancements.* These features include, for example, color highlighting of ballot choices and candidate pictures.

- *Accommodations for voters with disabilities.* Examples of options for voters who are blind include Braille keyboards and audio interfaces.[11] At least one vendor reported that its DRE accommodates voters with neurological disabilities by offering head movement switches and "sip and puff" plug-ins.[12] Another option is voice recognition capability, which allows voters to make selections orally.

- *An option to recover spoiled ballots.* This feature allows voters to recast their votes after their original ballots are cast. For this option, every DRE at the poll site could be connected to a local area network. A poll official would void the original "spoiled" ballot through the administrative workstation, which is also connected to the local area network. The voter could then cast another ballot.

- *An option to provide printed receipts.* This option, provided by a voter-verified paper audit trail system, provides the voter with a paper printout or ballot when the vote is cast. This feature is intended to provide voters and/or election officials with an opportunity to check what is printed against what is recorded and displayed.

HAVA Is Expected to Enhance the Federal Role in Election Processes

In October 2002, Congress passed the Help America Vote Act (HAVA) to provide states with organizations, processes, and resources for improving the administration of future federal elections. The act also specified time frames for the availability of these organizations, processes, and resources. The act was intended, among other things, to encourage states to upgrade antiquated voting systems and technologies and to support the states in making federally mandated improvements to their voting systems, such as ensuring that voters can verify their votes before casting their ballot, providing records for manual auditing of voting systems, and establishing maximum error rates for counting ballots.

[11]According to spokespersons for national advocacy groups for people with disabilities, only a small percentage of blind people have the Braille proficiency needed to vote using a Braille ballot.

[12]Using a mouth-held straw, the voter issues switch commands—hard puff, hard sip, soft puff, and soft sip—to provide signals or instructions to the voting machine.

Organizations. HAVA established the Election Assistance Commission (EAC) and gave this commission responsibility for activities and programs related to the administration of federal elections. This independent federal agency consists of four presidential appointees confirmed by the Senate, as well as support staff, including personnel inherited from the former Office of Election Administration of the Federal Election Commission. EAC commissioners were appointed in December 2003, and the commission began operations in January 2004. EAC is intended to serve as a national clearinghouse and resource for the compilation of information and procedures on election administration. Its responsibilities relative to voting systems include

- adopting and maintaining voluntary voting system guidelines;
- managing a national program for testing, certification, decertification, and recertification of voting system hardware and software;
- maintaining a clearinghouse of information on the experiences of state and local governments in implementing the guidelines and operating voting systems; and
- conducting studies and other activities to promote effective administration of federal elections.

HAVA also established three organizations and levied new requirements on a fourth to assist EAC in establishing voting system standards and performing its responsibilities, including standards and responsibilities involving the security and reliability of voting systems:

- The *Technical Guidelines Development Committee* (TGDC) is to assist EAC in developing voluntary voting system standards (which are now called guidelines). This committee includes selected state and local election officials and representatives of professional and technical organizations. It is chaired by the Director of the National Institute of Standards and Technology.
- The *Standards Board* brings together one state and one local official from each of the 55 states and territories to review the voluntary voting system guidelines developed by TGDC and provide comments and recommendations on the guidelines to EAC.

- The *Board of Advisors* is made up of 37 members—many from various professional and specialty organizations.[13] Like the Standards Board, the Board of Advisors reviews the voluntary voting system guidelines developed by TGDC and provides comments and recommendations to EAC.

- The Department of Commerce's *National Institute of Standards and Technology* (NIST) provides technical support to TGDC, including research and development of the voting system guidelines. NIST is also responsible for monitoring and reviewing the performance of independent testing laboratories (previously known as independent testing authorities) and making recommendations for accreditation and revocation of accreditation of the laboratories by EAC. NIST's responsibilities for improving the security and reliability of electronic voting systems include identification of security and reliability standards for voting system computers, networks, and data storage; methods to detect and prevent fraud; and protections for voter privacy and remote voting system access.

Processes. HAVA provides for three major processes related to the security and reliability of voting systems: updating voluntary standards, accrediting independent testing laboratories, and certifying voting systems to meet national standards. HAVA specifies the organizations involved, activities to be undertaken, public visibility for the processes, and, in some cases, work products and deadlines. These processes are described below.

- *Updating standards.* EAC and TGDC were given responsibility for evaluating and updating the Federal Election Commission's voluntary voting system standards of 2002. TGDC is to propose standards changes within 9 months of the appointment of all of its members, and EAC is to hold a public hearing and a comment period for the standards changes and allow at least 90 days for review and comment by the standards and

[13]The Board of Advisors includes scientific and technical experts appointed by Congress and representatives from the National Governors Association; the National Conference of State Legislatures; the National Association of Secretaries of State; the National Association of State Election Directors; the National Association of Counties; the National Association of County Recorders, Election Administrators, and Clerks; the United States Conference of Mayors; the Election Center; the International Association of County Recorders, Election Officials, and Treasurers; the United States Commission on Civil Rights; the Architectural and Transportation Barrier Compliance Board; the Office of Public Integrity of the Department of Justice; the Voting Section of the Department of Justice's Civil Rights Division; and the Federal Voting Assistance Program of the Department of Defense.

advisory boards before voting on the standards. EAC and its boards are also to consider updates to the standards on an annual basis.

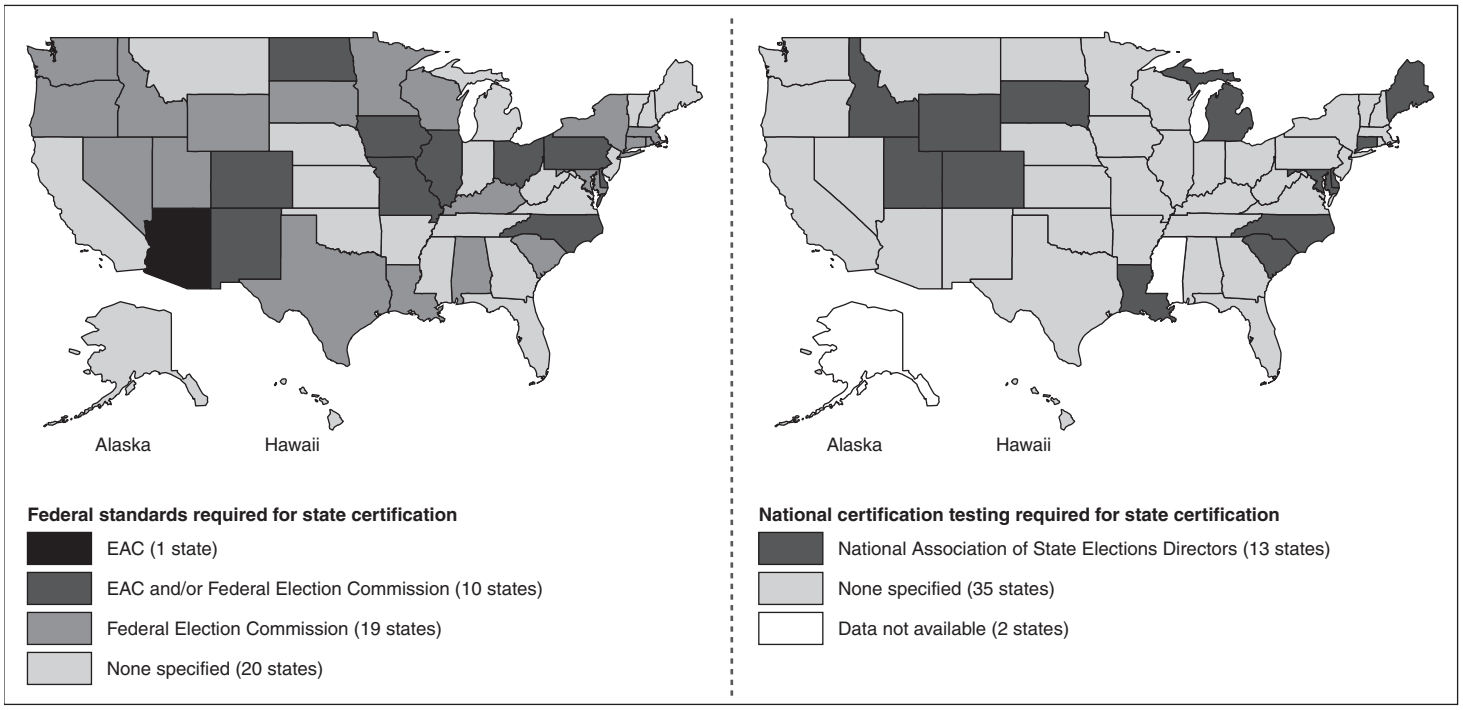
- *Accrediting laboratories.* NIST's director is charged with evaluating the capabilities of independent nonfederal laboratories to carry out certification testing of voting systems within 6 months after EAC adopts the first update to the voluntary voting system standards.[14] Through its National Voluntary Laboratory Accreditation Program, NIST is to recommend qualified laboratories for EAC's accreditation, provide ongoing monitoring and reviews of the accredited laboratories, and recommend revocation of accreditation, if necessary.

- *Certifying systems.* EAC is to establish processes for certifying, decertifying, and recertifying voting systems. HAVA allows the current processes (as conducted under the National Association of State Election Directors) to continue until the laboratory accreditation processes to be developed by NIST are established and laboratories are accredited by EAC to conduct certification testing. States may also use the nationally accredited testing laboratories for testing associated with certification, decertification, and recertification of voting systems to meet state certification requirements.

The majority of states currently rely on federal standards, but do not require national certification testing to ensure that voting systems meet functional, performance, and quality goals. On the basis of an April 2005 review of state statutes and administrative rules, EAC identified at least 30 states that require their voting systems to meet federal standards issued by the Federal Election Commission, EAC, or both (see fig. 4). As for certification, the majority of states require state certification of voting systems, but do not require national testing. Only 13 states currently require their systems to be tested against the federal standards by independent testing authorities and certified by the National Association of State Election Directors (see fig. 4). In commenting on a draft of this report, EAC noted that some state and local jurisdictions can choose to exceed state statute and administrative rules—and may be using federal standards and national certification testing.

[14]These standards are fundamental to identifying the capabilities that the laboratories must possess.

Figure 4: States Requiring the Use of Federal Voting System Standards and States Requiring National Certification Testing



Source: GAO analysis of EAC data.

Note: State requirements are based on EAC assessment of state statute and administrative rule.

Resources. HAVA authorized federal payments to help states improve their voting systems in two ways:

- By replacing punch card and lever voting systems in time for the November 2004 federal election unless a waiver authorizing a delay is granted by the Administrator of the General Services Administration. In the event of a waiver, states are required to replace the systems in time for the first federal election held after January 1, 2006.[15] EAC reports that approximately $300 million was distributed to 30 states under this HAVA provision—all in fiscal year 2003.

[15]Section 102, Help America Vote Act (Oct. 29, 2002).

- By incorporating new voting system functions required by HAVA (for instance, ballot verification by voters, producing printed records for election auditing, and meeting vote counting error rates);[16] upgrading systems in general; improving the administration of elections; or educating voters and training election workers (among other things).[17] EAC reported that as of August 31, 2005, approximately $2.5 billion had been disbursed to the 50 states, 4 U.S. territories, and the District of Columbia, for these and other election improvements.

Time frames. HAVA specifies time frames for several key activities. Specifically, it requires that

- EAC commissioners be appointed no later than 120 days after the law was enacted,
- a program to distribute payments to states to replace antiquated voting systems be in place no later than 45 days after the law was enacted,
- the first set of recommendations for revising the voluntary voting system standards be submitted to EAC no later than 9 months after the appointment of TGDC members,
- EAC approve voluntary guidance for certain voting system standards by January 2004,
- NIST conduct evaluations of independent testing laboratories for accreditation within 6 months of the adoption of updated voting standards,
- states receiving federal payments replace their lever or punch card voting machines in time for the November 2004 federal election, or the first federal election after January 2006, with a waiver, and
- states meet requirements for federally mandated improvements to voting systems, such as voter verification of ballots, records for manual audits, and maximum error rates for ballot counts (HAVA Section 301) by January 1, 2006.

[16]Sections 101 and 251, Help America Vote Act (Oct. 29, 2002).

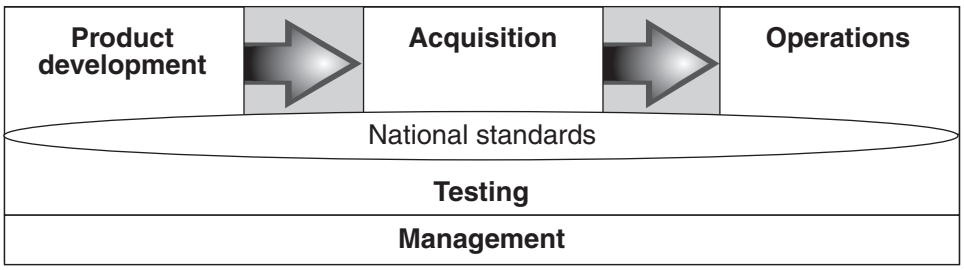
[17]Section 101, Help America Vote Act (Oct. 29, 2002).

EAC commissioners were appointed in December 2003—over a year after the law was enacted—and the commission began operations in January 2004. It received $1.2 million in funding in fiscal year 2004 increasing to $14 million in fiscal year 2005. Thus, the commission got a late start on its initiatives. As discussed later in this report, key activities are currently under way.

Security and Reliability Are Important Elements Throughout the Voting System Life Cycle

Electronic voting systems are typically developed by vendors and then purchased commercially off the shelf and operated by state and local election administrators. Viewed at a high level, these activities make up three phases of a system life cycle: product development, acquisition, and operations (see fig. 5). Key processes that span these life cycle phases include managing the people, processes, and technologies within each phase, and testing the systems and components during and at the end of each phase. Additionally, voting system standards are important through all of the phases because they provide criteria for developing, testing, and acquiring voting systems, and they specify the necessary documentation for operating the systems. As with other information systems, it is important to build principles of security and reliability into each phase of the voting system life cycle.

Figure 5: A Voting System Life Cycle Model



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

The *product development* phase includes activities such as establishing requirements for the system, designing a system architecture, and developing software and integrating components. Activities in this phase are performed by the system vendor. Design and development activities related to security and reliability of electronic voting systems include such things as requirements development and hardware and software design.

The *acquisition* phase covers activities for procuring voting systems from vendors such as publishing a request for proposal, evaluating proposals, choosing a voting technology, choosing a vendor, and writing and administering contracts. For voting systems, activities in this phase are primarily the responsibility of state and local governments, but entail some responsibilities that are shared with the system vendor (such as establishing contractual agreements). Acquisition activities affecting the security and reliability of electronic voting systems include such things as specifying provisions for security controls in contracts and identifying evaluation criteria for prospective systems.

The *operations* phase consists of activities for operating the voting systems, including the setup of systems before voting, vote capture and counting during elections, recounts and system audits after elections, and storage of systems between elections. Responsibility for activities in this phase typically resides with local jurisdictions. Security and reliability aspects of this phase include physical security of the polling place and voting equipment, chain of custody for voting system components and supplies, system audit logs and backups, and the collection, analysis, reporting, and resolution of election problems.

Standards for voting systems were developed at the national level by the Federal Election Commission in 1990 and 2002 and are now being updated by EAC, TGDC, and NIST. Voting system standards affect all life cycle phases. In the product development phase, they serve as guidance for developers to build systems. In the acquisition phase, they provide a framework that state and local governments can use to evaluate systems. In the operations phase, they specify the necessary documentation for operating the systems. Current and planned national standards include explicit requirements for ensuring the security and reliability of voting systems.

Testing processes are conducted throughout the life cycle of a voting system. Voting system vendors conduct product testing during development of the system and its components. National testing of products submitted by system vendors is conducted by nationally accredited independent testing authorities. States may conduct evaluation testing before acquiring a system to determine how well products meet their specifications, or may conduct certification testing to ensure that a system performs its functions as specified by state laws and requirements. Once a voting system is delivered by the system vendor, states and local jurisdictions may conduct acceptance testing to ensure that the system

satisfies functional requirements. Finally, local jurisdictions typically conduct logic and accuracy tests related to each election, and sometimes subject portions of the system to parallel testing during each election to ensure that the system components perform accurately. All of these tests should address system security and reliability.

Management processes ensure that each life cycle phase produces desirable outcomes. 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. These activities are conducted by the responsible parties in each life cycle phase. Management processes related to security and reliability include program planning, disaster recovery and contingency planning, definition of security roles and responsibilities, configuration management of voting system software and hardware, and poll worker security training.

In 2004, we reported that the performance of electronic voting systems, like any type of automated information system, can be judged on several bases, including how well its design provides for security, accuracy, ease of use, efficiency, and cost.[18] We also reported that voting system performance is a function of how it was designed and developed, whether the system performs as designed, and how the system is implemented. In implementing a system, it is critical to have people with the requisite knowledge and skills to operate it according to well-defined and understood processes.

Significant Concerns Have Been Raised about the Security and Reliability of Electronic Voting Systems

Electronic voting systems hold promise for improving the efficiency and accuracy of the election process by automating a manual process, providing flexibility for accommodating voters with special needs, and implementing controls to avoid errors by voters and election workers. However, in a series of recent reports, election officials, computer security experts, citizen advocacy groups, and others have raised significant concerns about the security and reliability of electronic voting systems, citing instances of weak security controls, system design flaws, inadequate system version control, inadequate security testing, incorrect system configuration, poor security management, and vague or incomplete

[18]GAO, *Elections: Electronic Voting Offers Opportunities and Presents Challenges*, GAO-04-975T (Washington, D.C.: July 20, 2004).

standards, among other issues. Most of the issues can be viewed in the context of the voting system life cycle, including (1) the development of voting systems, including the design of these systems and the environments in which they were developed; (2) the nature and effectiveness of the testing program for electronic voting systems; (3) the operation and management of electronic voting systems at the state and local levels; and (4) the voluntary voting systems standards, which govern different activities at different phases. The aspects of the life cycle are interdependent—that is, a problem experienced in one area of the life cycle will likely affect the other areas. For example, a weakness in system standards could result in a poorly designed system during the development phase, which then malfunctions in the operational phase. Also, each of the life cycle phases depends on the management of people, processes, and technology to ensure that they are executed in a manner that adequately ensures reliable and secure results. Because of these multiple interdependencies, it is sometimes difficult to determine the root cause of some problems. Table 1 provides a summary of the different types of concerns identified.

In viewing these concerns, it is important to note that many involved vulnerabilities or problems with specific voting system makes and models or circumstances in a specific jurisdiction's election, and that there is a lack of consensus among elections officials, computer security experts, and others on the pervasiveness of the concerns. Nevertheless, there is evidence that some of these concerns have been realized and have caused problems with recent elections, resulting in the loss and miscount of votes. In light of the recently 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, the security and reliability concerns raised in recent reports merit the focused attention of federal, state, and local authorities responsible for election administration.

Table 1: Common Types of Security and Reliability Concerns Viewed in Terms of the Voting System Life Cycle

Life cycle component	Common concerns
Product development	• Weak system security controls • Design flaws in voter-verified paper audit trail systems • Weak security management practices
Acquisition	No significant concerns reported
Operations	• Incorrect system configuration • Poor implementation of security procedures • System failures during elections
Standards	• Vague and incomplete security provisions • Inadequate provisions for commercial off-the-shelf systems and telecommunications and networking services • Inadequate requirements for vendor documentation
Testing	• Inadequate security testing • Lack of transparency in the testing process
Management	• Poor version control of system software • Inadequate security management

Source: GAO analysis and summary.

Common concerns as well as examples of the problems identified during recent elections are discussed in more detail below.

Product Development

Multiple recent reports, including several state-commissioned technical reviews and security assessments, voiced concerns about the development of secure and reliable electronic voting systems by system vendors. Three major areas of concern are weak security controls, audit trail design flaws, and weak security management practices.

Weak system security controls. Some electronic voting systems provided weak system security controls over key components (including electronic storage for votes and ballots, remote system access equipment, and system event and audit logs), access to the systems, and the physical system hardware.

- Regarding key software components, several evaluations demonstrated that election management systems did not encrypt the data files containing cast votes (to protect them from being viewed or modified).[19] Evaluations also showed that, in some cases, other computer programs could access these cast vote files and alter them without the system recording this action in its audit logs.[20] Two reports documented how it might be possible to alter the ballot definition files on one model of DRE so that the votes shown on the touch screen for one candidate would actually be recorded and counted for a different candidate.[21] In addition, one of these reports found that it was possible to gain full control of a regional vote tabulation computer—including the ability to modify the voting software—via a modem connection.[22] More recently, computer security experts working with a local elections supervisor in Florida demonstrated that someone with physical access to an optical scan voting system could falsify election results without leaving any record of this action in the system's audit logs by using altered memory cards.[23] If exploited, these weaknesses could damage the integrity of ballots, votes, and voting system software by allowing unauthorized modifications.

[19]See bibliographical (bib.) entries 2, 3, 5, and 21. Numbers refer to primary sources listed in the bibliography. Information presented is based on both primary sources and supplementary information gathered from other reports, public testimonies, and interviews with experts.

[20]See bib. entries 2, 7, 21, and 25.
Elections and other officials said that there has never been a proven case of fraud involving tampering with electronic voting systems. If, however, an attacker (for instance, a malicious insider) exploited this particular flaw, such tampering would be difficult to notice and to prove.

[21]See bib. entries 13 and 21.
Ballot definition files are not subject to testing by independent testing authorities.

[22]See bib. entry 21.

[23]See bib. entry 7.

- Regarding access controls, many security examinations reported flaws in how controls were implemented in some DRE systems.[24] 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.[25] In another case, the same personal identification number was programmed into all supervisor cards nationwide—meaning that the number was likely to be widely known.[26] Reviewers also found that values used to encrypt election data (called encryption keys) were defined in the source code.[27] Several reviews reported that smart cards (used to activate the touch screen on DRE systems) and memory cards (used to program the terminals of optical scan systems) were not secured by some voting systems. Reviewers exploited this weakness by altering such cards and using them to improperly access administrator functions, vote multiple times, change vote totals, and produce false election reports in a test environment.[28] Some election officials and security experts felt that physical and procedural controls would detect anyone attempting to vote multiple times during an actual election.[29] Nevertheless, in the event of lax supervision, the privileges available through these access control flaws could allow unauthorized personnel to disrupt operations or modify data and programs that are crucial to the accuracy and integrity of the voting process.

[24]See bib. entries 2, 3, 7, 13, 19, 21, and 22.

[25]See bib. entries 2 and 21.

[26]See bib. entry 2.

[27]See bib. entries 2 and 13.

[28]See bib. entries 7, 13, and 21.

[29]See bib. entries 19, 22, and 26.

- Regarding physical hardware controls, several recent reports found that many of the DRE models under examination contained weaknesses in controls designed to protect the system. For instance, one report noted that all the locks on a particular DRE model were easily picked, and were all controlled by the same keys—keys that the reports' authors were able to copy at a local store.[30] However, the affected election officials felt that this risk would be mitigated by typical polling-place supervisors, who would be able to detect anyone picking the lock on a DRE terminal.[31] In another report, reviewers were concerned that a particular model of DRE was linked together with others to form a rudimentary network.[32] If one of these machines were 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.[33]

[30]See bib. entry 21.

[31]See bib. entry 26.

[32]See bib. entry 2.

[33]See bib. entry 2.

Design flaws in the voter-verified paper audit trail systems. Voter-verified paper audit trail systems involve adding a paper printout to a DRE system that a voter can review and verify. Some citizen advocacy groups, security experts, and elections officials advocate these systems as a protection against potential DRE flaws.[34] However, other election officials and researchers have raised concerns about potential reliability and security flaws in the design of such systems.[35] Critics of the systems argue that adding printers increases the chance of mechanical failure and disruption to the polling place.[36] Critics also point out that these systems introduce security risks involving the paper audit trail itself. Election officials would need to safeguard the paper ballots. 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.[37] If not protected, such information could breach voter confidentiality.

[34]See bib. entries 13 and 19; information supplemented by interviews.

[35]See bib. entries 18 and 23.

[36]See bib. entry 23; information supplemented by interviews.

[37]Refer to public discussions at TGDC meetings on January 18–19, 2005 (http://www.eastbaymedia.com/tgdc-webcast/) and March 29, 2005 (http://www.eastbaymedia.com/tgdc-march/).

Weak security management practices. Selected state elections officials, computer security experts, and election experts view the reported instances of weak controls as an indication that the voting system vendors lack strong security management and development practices.[38] Security experts and local election officials cite the position of trust that vendors occupy in the overall election process, and say that to ensure the security and reliability of electronic voting systems—as well as improve voters' confidence in the electoral process—vendors' practices need to be above reproach.[39] Specific concerns have been expressed about (1) the personnel security policies used by vendors, including whether vendors conduct background checks on programmers and systems developers; (2) whether vendors have established strict internal security protocols and have adhered to them during software development; and (3) whether vendors have established clear chain of custody procedures for handling and transporting their software securely.[40] A committee of election system vendors generally disagrees with these concerns and asserts that their security management practices are sound.

Election Operations

Several reports raised concerns about the operational practices of local jurisdictions and the performance of their electronic voting systems during elections. These include incorrect system configurations, poor implementation of security procedures, and operational failures during an election.

Incorrect system configuration. Some state and local election reviews have documented cases in which local governments did not configure their voting systems properly for an election. For instance, a county in California presented some voters with an incorrect electronic ballot in the March 2004 primary.[41] As a result, these voters were unable to vote on certain races. In another case, a county in Pennsylvania made a ballot programming error on its DRE system.[42] This error contributed to many votes not being

[38]See bib. entries 13 and 18; information supplemented by interviews.

[39]See bib. entry 18; information supplemented by interviews.

[40]See bib. entries 14, 18, and 19.

[41]See bib. entry 19.

[42]See bib. entries 4 and 25.

captured correctly by the voting system, evidenced by that county's undervote percentage, which reached 80 percent in some precincts.

Poor implementation of security procedures. Several reports indicated that state and local officials did not always follow security procedures. Reports from Maryland 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 exposing the system to general security threats.[43] In another example, election monitors in Florida described how certain precincts did not ensure that the number of votes matched the number of signatures on the precinct sign-in sheets, thus raising questions as to whether the voting systems captured the correct number of votes.[44] A report from California cited a number of counties that failed to follow mandatory security measures set forth by the Secretary of State's office that were designed to compensate for potential security weaknesses in their electronic voting systems.[45]

[43]See bib. entries 21 and 22.

[44]See bib. entry 16.

[45]See bib. entry 19.

System failures during elections. Several state and local jurisdictions have documented instances when their electronic voting systems exhibited operational problems during elections. For example, California officials documented how a failure in a key component of their system led to polling place disruptions and an unknown number of disenfranchised voters.[46] In another instance, DRE voting machines in one county in North Carolina continued to accept votes after their memories were full, effectively causing over 4,000 votes to be lost.[47] The same system was used in Pennsylvania, where the state's designated voting system examiner noted several other problems, including the system's failure to accurately capture write-in or straight ticket votes, screen freezes, and difficulties sensing voters' touches.[48] A Florida county experienced several problems with its DRE system, including instances where each touch screen took up to 1 hour to activate and had to be activated separately and sequentially, causing delays at the polling place.[49] In addition, election monitors discovered that the system contained a flaw that allowed one DRE system's ballots to be added to the canvass totals multiple times without being detected.[50] In another instance, a malfunction in a DRE system in Ohio caused the system to record approximately 3,900 votes too many for one presidential candidate in the 2004 general election.[51] While each of these problems was noted in an operational environment, the root cause was not known in all cases.

Standards

In 1990, the Federal Election Commission issued a set of voluntary voting systems standards, which were later revised in 2002. These standards identify minimum functional and performance requirements for electronic voting systems such as optical scan and DRE voting equipment. The functional and performance requirements address what voting equipment should do and delineate minimum performance thresholds, documentation

[46]See bib. entry 19.

[47]See bib. entry 25.

[48]See bib. entry 25. Pennsylvania has since decertified this system.

[49]See bib. entries 9 and 17.

[50]See bib. entry 16. The report also notes that several supervisory procedures were not followed at this precinct, which contributed to the counting problems.

[51]See bib. entry 6.

provisions, and security and quality assurance requirements. These standards also specify testing to ensure that the equipment meets these requirements. The standards are voluntary—meaning that states are free to adopt them in whole or in part, or reject them entirely.

Computer security experts and others have criticized the 2002 voting system standards for not containing requirements sufficient to ensure secure and reliable voting systems. Common concerns with the standards involve vague and incomplete security provisions, inadequate provisions for some commercial products and networks, and inadequate documentation requirements.

Vague and incomplete security provisions. Security experts and others have criticized the security provisions in the voting system standards for being vague and lacking specific requirements.[52] Although the standards require the presence of many kinds of security controls, the concern is that they are not specific enough to ensure the effective and correct implementation of the controls. One of the independent testing authorities agreed and noted that the broad terms of the standards do not provide for consistent testing because they leave too much room for interpretation.[53]

Computer security and testing experts have also noted that the current voting system standards are not comprehensive enough and that they omit a number of common computer security controls. For example, an independent testing authority expressed a concern that the standards do not prohibit many software coding flaws, which could make the voting system software susceptible to external attack and malicious code.[54] In addition, NIST performed a review of the voting system standards and found numerous gaps between its own security guidance for federal information systems and those prescribed by the standards. Others have argued that the standards are simply out of date, and contain no guidance

[52]See bib. entries 12, 15, and 27.

[53]See bib. entry 1; information supplemented by interview.

[54]See bib. entry 1.

on technologies such as wireless networking and voter-verified paper audit trails. [55]

Inadequate provisions for commercial off-the-shelf (COTS) systems and telecommunications and networking services. Computer security experts have raised concerns about a provision in the voting system standards that exempts 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 like Microsoft Windows. 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.[56] Regarding telecommunication 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 guarantee their security and reliability—even with safeguards such as encryption and digital signatures in place.[57]

Inadequate requirements for documentation. Computer security experts and some elections officials have expressed concerns that the documentation requirements in the voting system standards are not explicit enough. For instance, computer security experts warn that the documentation requirements for source code are not sufficient for code that is obscure or confusing, nor do they require developers to sufficiently map out how software modules interact with one another.[58] This could make it difficult for testers and auditors to understand what they are reviewing, lessening their ability to detect unstable or hidden (and potentially malicious) functionality. In addition, election officials and a security expert raised concerns that the standards do not require sufficient

[55]See bib. entries 10 and 24; information supplemented by public discussion at the TGDC meeting of March 29, 2005 (http://www.eastbaymedia.com/tgdc-march/). According to EAC officials, the commission plans to address some of these omissions in the new voluntary system guidelines currently under review.

[56]See bib. entries 10, 12, 15, and 18.

[57]See bib. entries 15 and 27; information supplemented by public discussion at TGDC meeting on January 18–19, 2005 (http://www.eastbaymedia.com/tgdc-webcast/).

[58]See bib. entries 11 and 15.

documentation for local officials with respect to proper operation and maintenance procedures.[59] For instance, election officials in one state noted that when voting machines malfunctioned and started generating error messages during an election, state technicians were unable to diagnose and resolve the problems because the vendor's documentation provided no information about what the error messages meant, or how to fix the problems.[60]

Voting System Testing

Security experts and some election officials have expressed concerns that tests currently performed by independent testing authorities and state and local election officials do not adequately assess electronic voting systems' security and reliability. These concerns are amplified 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 functional testing, source code reviews, and penetration testing.[61] Illustrating their concerns, most of the systems with weak security controls identified earlier in this report (see product development issues) had previously been certified by the National Association of State Election Directors 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.

- Regarding the functional testing conducted by independent testing authorities and state and local officials, election and security experts expressed concern that this testing may not reveal certain security flaws in electronic voting systems.[62] They argue that functional tests only

[59]See bib. entries 15 and 19.

[60]See bib. entry 19.

[61]See bib. entries 12, 15, 21, and 27; information supplemented by public discussions at the TGDC meeting on January 18–19, 2005 (http://www.eastbaymedia.com/tgdc-webcast/). Functional testing is done to ensure that the system performs as expected under normal conditions. Source code reviews involve an assessment of the code to ensure that it complies with the 2002 voting system standards and that there are no hidden functions. Penetration testing involves testers attempting to circumvent the security controls of a system.

[62]See bib. entries 12, 19, and 27.

measure a system's performance when it is used as expected, under normal operating conditions.[63] As a result, this testing cannot determine what might happen if a voter acts in unexpected ways, or how the system would react in the face of an active attack. Specifically, security experts argue that functional testing is unlikely to ever trigger certain types of hidden code.[64] As a result, malicious code could be present in a system and evade testing as long as the triggering commands were not entered.

- Security and testing experts also expressed concern that the source code reviews called for in the voting system standards and conducted by independent testing authorities are too general and do not take into account the unique nature of voting systems. For instance, several experts noted that malicious code could be hidden in source code and be obscure enough to avoid detection by the general reviews, which currently focus on coding conventions, comments, and line length.[65] Moreover, there is concern that these code reviews may not adequately inspect how voting system software interacts with key election data.[66] Specifically, security experts say that a testing authority's source code review should include checks for unique elements of the election contest, including (1) software modules with inappropriate access to vote totals, ballot definition files, or individual ballots; (2) functionality with time or date dependent behavior; and (3) software modules that retain information from previous screen touches or previous voters—all potentially indicative of improper and malicious voting system behavior.[67]

- As for penetration testing, experts expressed concerns that voting system testing does not include such explicit security tests.[68] An official from an independent testing authority generally agreed and said that the security-related parts of their testing use a checklist approach, based on

[63]See bib. entries 12 and 27.

[64]See bib. entries 12 and 27.

[65]See bib. entries 1, 12, and 27.

[66]See bib. entries 12 and 15.

[67]See bib. entry 12; information supplemented by interviews.

[68]See bib. entries 15, 21, and 27; information supplemented by interviews.

what is called for in the voluntary voting system standards. This official recommended more rigorous security testing. Another testing authority official said that their testing does not guarantee that voting systems are secure and reliable. This official has called for local jurisdictions to conduct additional security testing and risk analyses of their own.[69]

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.[70] (Designated election officials may, in fact, obtain copies of test results for their systems, but only with the permission of the vendor.) As a result, critics argue, the rigor of the testing process is largely unknown. Critics say that this lack of transparency hinders oversight and auditing of the testing process.[71] 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,[72] one security expert noted that a system should be secure enough to resist even a knowledgeable attacker.[73]

Security Management

Numerous studies raised concerns about the security management practices of state and local governments in ensuring the security of electronic voting systems, citing poor version control of system software and inadequate security management programs.

Poor version control of system software. Security experts and selected election officials are concerned about the configuration management practices of state and local jurisdictions. Specifically, the voting system software installed at the local level may not be the same as what was

[69]Information obtained from interviews.

[70]See bib. entry 24; information supplemented by interview.

[71]See bib. entries 18 and 24; information supplemented by interviews.

[72]See bib. entry 21; information supplemented by public discussion at the TGDC meeting of March 29, 2005 (http://www.eastbaymedia.com/tgdc-march/) and interview.

[73]Information obtained from interview.

qualified and certified at the national or state levels.[74] These groups raised the possibility that either intentionally or by accident, voting system software could be altered or substituted, or that vendors or local officials might (knowingly or not) install untested or uncertified versions of voting systems.[75] As a result, potentially unreliable or malicious software might be used in elections. For example, in separate instances in California and Indiana, state officials found that two different vendors had violated regulations and state law by installing uncertified software on voting systems.[76]

Inadequate security management programs. Several of the technical reviews mentioned previously also found that states did not have effective information security management plans in place to oversee their electronic voting systems.[77] 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 configure their voting system audit logs and require them to be reviewed.

In addition, several reports indicated that *s*ome state and local jurisdictions did not always have procedures in place to address problems with their electronic voting systems.[78] For instance, one county in Pennsylvania reported that neither its election staff nor its technical division knew how to deal with several problems that occurred on election day.[79] The report also cited (1) a lack of preparation and contingency planning for significant problems, (2) inadequate communication means between precincts and the county election office for problem reporting, and (3) the absence of paper ballots held in reserve as a backup. In addition, this and other reports indicated that poll workers might not receive sufficient training, or possess

[74]See bib. entries 1, 22, and 24.

[75]See bib. entries 20 and 24.

[76]See bib. entries 14 and 20.

[77]See bib. entries 2, 8, and 22.

[78]See bib. entries 4, 16, and 19.

[79]See bib. entry 4.

adequate technical skills or knowledge of their particular systems to manage, administer, and troubleshoot them.[80]

While the concerns listed above are numerous, it is important to note that many involved problems with specific voting system makes and models or with circumstances in a specific jurisdiction's election. Further, there is a lack of consensus among election officials, computer security experts, and others on the pervasiveness of the concerns. On one hand, both vendors and election officials express confidence in the security of their current products. Election officials note that their administrative procedures can compensate for inherent system weaknesses, and they point out that there has never been a proven case of fraud involving tampering with electronic voting systems. Alternatively, citizen groups and computer security experts note that administrative procedures cannot compensate for all of the weaknesses and that if electronic voting system security weaknesses are exploited, particularly by those with insider access to the systems, changes to election results could go undetected.[81]

Nevertheless, there is evidence that some of these concerns—including weak controls and inadequate testing—have caused problems with recent elections, resulting in the loss and miscount of votes. In light of the recently 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, the security and reliability concerns raised in recent reports merit attention.

Recommended Practices Address Electronic Voting Systems' Security and Reliability

Several federal, academic, and nongovernmental organizations have issued guidance to help state and local election officials improve the election and voting processes. This guidance includes recommended practices for enhancing the security and reliability of voting systems. For example, in mid-2004, EAC issued a compendium of practices recommended by

[80]See bib. entries 4, 16, and 19.

[81]Several of the reports we reviewed offered suggestions to address identified weaknesses. These are summarized in appendix II, table 6.

elections experts, including state and local jurisdictions.[82] This compendium, among many suggested practices, includes activities to help ensure a secure and reliable voting process throughout a voting systems' life cycle. As another example, in July 2004, the California Institute of Technology and the Massachusetts Institute of Technology issued a report recommending immediate steps to avoid lost votes in the 2004 election, including suggestions for testing equipment, retaining audit logs, and physically securing voting systems.[83]

In addition to this election-specific guidance, the federal government and other entities have published extensive guidance intended to help organizations address, evaluate, and manage the security and reliability of their information technology systems. This guidance includes practices in the product development phase of the system life cycle that may assist voting system vendors in adopting appropriate standards and practices for designing and developing secure and reliable voting systems. In addition, this guidance includes practices in the areas of acquisition, testing, operation, and management that may help state governments and local election officials in acquiring technologies and services; assessing security risks; selecting, applying, and monitoring security controls; auditing systems; and adopting security policies.

The following is a high-level summary of common practices identified in both general and election-specific reports that address the security and reliability of electronic voting systems in the context of the system life cycle phases and cross-cutting activities. The recommended practices in both election-specific and IT-focused guidance documents provide valuable guidance throughout a voting system's life cycle that, if implemented effectively, should help improve the security and reliability of voting systems. Appendix II provides a more detailed summary of the election-specific publications' guidance on voting system security and reliability practices, and appendix III provides summaries of general guidance on information systems security.

[82]EAC. *Best Practices Tool Kit* (July 2004), http://www.eac.gov/bp/docs/BestPracticesToolKit.doc (downloaded Oct. 1, 2004).

[83]California Institute of Technology/Massachusetts Institute of Technology Voting Technology Project. *Immediate Steps to Avoid Lost Votes in the 2004 Presidential Elections: Recommendations for the Election Assistance Commission* (Pasadena, Calif., July 2004). http://www.vote.caltech.edu/media/ documents/EAC.pdf (downloaded Oct. 1, 2004).

Product Development

- Voting system developers should define security requirements and specifications early in the design and development process.
- The security requirements for voting systems should consider the unique security needs of elections and the voting environment, as well as applicable laws, national standards, and other external influences and constraints that govern systems.
- Voting systems should contain audit logs that record all activity involving access to and modifications of the system, particularly of sensitive or critical files or data, including the time of the event, the type of event and its result, and the user identification associated with the event.
- Voting systems should employ adequate logical access controls over software and data files. Systems should require that passwords be changed periodically, and that they not use names or words from the dictionary. Further, the use of vendor-supplied or generic passwords should be prohibited.
- Vendors should review lessons learned from recent elections and implement relevant mitigation steps to address known security weaknesses (see app. II, table 16).

Acquisition

- Election officials should focus on the security issues related to electronic voting equipment before purchasing or implementing voting systems.
- Requests for proposals should include security requirements and evaluation and test procedures.
- Election officials should review lessons learned from recent elections and implement relevant mitigation steps to address known security weaknesses (see app. II, table 16).

Operations

- State and local authorities should ensure that sensitive activities in the election process, such as vote tabulation and the transporting of ballots or election results, are performed by more than one person or observed by representatives of both major parties.

	• Procedures should be developed and followed to identify and document the chain of custody for every instance when sensitive election items (such as memory cards, ballots, and voting machines) change hands. • Voting machines, ballots, memory cartridges, election supplies, and offices should be physically secured against unauthorized access before, during, and after an election. • A postelection audit of voting systems should be conducted to reconcile vote totals and ballot counts, even if there is no recount scheduled. • An audit of the election system and process should be conducted after election day to verify that the election was conducted correctly and to uncover any evidence of security breaches or other problems that may not have surfaced on election day.
Standards	• States should adopt the most current version of the national voluntary voting standards or guidelines.
Testing	• During the product development phase, electronic voting system developers should verify and validate the security controls on the system before deployment in order to ensure that the controls are working properly and effectively and that they meet the operational security needs of the purchasing jurisdiction. • During the acquisition phase, states and local governments should require that voting systems be certified against federal standards. • During the operations phase, localities should conduct logic and accuracy testing on voting machines before the election to ensure that they accurately record votes.
Management	• Voting system developers should establish a sound security policy that identifies the security goals of their system; the procedures, standards, and controls needed to support the system security goals; the critical assets; and the security-related roles and responsibilities.

- Voting system developers should conduct appropriate background screening on all employees before granting them access to sensitive information or placing them into sensitive positions.

- Election officials should plan for poll worker training early in the process and ensure that all training classes and materials include information on the security of voting systems and on election security procedures.

- Election officials, not vendors, should control the administration and use of the voting equipment. To that end, the election administration team should include persons with expertise in both computer security and voting system oversight.

- Election officials should conduct a risk analysis of voting systems and address any identified vulnerabilities and points of failure in the election process.

- Election officials should ensure that vendors provide tested and certified versions of voting system software by requiring that software be submitted to NIST's National Software Reference Library, and by verifying that the systems, including hardware, software, and software patches, have met all required standards through required testing.[84]

- Procedures and plans should be established for handling election day equipment failure, including backup and contingency plans. If voting machines malfunction during voting, they should not be repaired or removed from the polling place on election day.

[84]Election officials can verify that systems have met standards by requesting test reports from the testing laboratories and assessing the test results.

National Initiatives Are Under Way to Improve Voting System Security and Reliability, but Key Activities Need to Be Completed

Since the implementation of HAVA in 2002, the federal government has begun a range of actions that are expected to improve the security and reliability of electronic voting systems. EAC, with the support of TGDC and NIST, is in the process of updating voluntary voting system standards, is establishing federal processes to accredit independent test laboratories and certify voting systems to national standards, and is supporting state and local election management by providing a library for certified software and acting as a clearinghouse for information on voting system problems and recommended election administration and management practices. However, a majority of these efforts either lack specific plans for implementation in time to affect the 2006 general election or are not expected to be completed until after the 2006 election. As a result, it is unclear when these initiatives will be available to assist state and local election officials. In addition to the federal government's activities, nongovernmental initiatives are under way to (1) define international voting system standards; (2) develop designs for open voting system products; (3) provide a framework of acquisition questions to use in acquiring voting systems; and (4) support management of voting systems by collecting and analyzing problem reports.

Federal Initiatives to Improve Voting Systems Security and Reliability Are Under Way

EAC, in collaboration with NIST and TGDC, has initiated efforts on several of its key responsibilities relating to the security and reliability of electronic voting systems, including improving voting system standards, developing a process to facilitate testing systems against the standards, and supporting state and local governments' election management. Table 2 summarizes federal initiatives—both those required by HAVA and those initiated by EAC to support HAVA requirements.

Table 2: Federal Initiatives Related to Improving the Security and Reliability of Voting Systems

Initiative	Responsibility	Status	Actual or planned completion date
Standards			
Draft initial set of voluntary voting system guidelines *(HAVA)*	TGDC	Completed	May 2005 (actual)
Adopt voluntary guidance for certain voting system standards *(HAVA)*	EAC	In process	Fall 2005
Complete security and reliability updates to voting system guidelines	TGDC recommends; EAC approves	In process	Not determined
Testing			
Conduct evaluation of independent testing laboratories for accreditation *(HAVA)*	NIST	Not yet initiated	By early 2007
Accredit first cadre of independent voting system testing laboratories *(HAVA)*	NIST recommends; EAC approves	Not yet initiated	By early 2007
Define interim process for certification of voting systems	EAC	In process	Fall 2005
Establish national program for voting system certification *(HAVA)*	EAC	In process	Not determined
Management support			
Establish national reference library for certified voting system software	NIST	Completed	July 2004 (actual)
Establish procedures for sharing problems associated with voting systems	NIST recommends; EAC approves	In process	Not determined
Provide an initial report that includes best practices for secure and reliable voting systems	EAC	Completed	August 2004 (actual)
Provide periodic reports on election administration practices *(HAVA)*	EAC	In process	First report by December 2006; later reports not determined

Source: GAO analysis of HAVA and EAC, NIST, and TGDC data.

Note: Initiatives followed by (*HAVA*) are required by the Help America Vote Act.

Standards. TGDC and NIST have been working on behalf of EAC to improve the 2002 Federal Election Commission voluntary voting system standards[85] and their impact on the acquisition, testing, operations, and management processes of the voting system life cycle.[86] TGDC approved 41

[85]The 2005 improvements to the voluntary voting system standards will be named the Voluntary Voting System Guidelines.

[86]Help America Vote Act of 2002, Sections 202 (1) and 221 (b).

resolutions between July 2004 and April 2005, many of which directed NIST to research and develop recommendations for changing various voting system capabilities and assurance processes. Of the 41 resolutions, 24 relate to the security and reliability of voting systems. Appendix IV contains the relevant resolutions and their status.

TGDC's initial priorities have been to correct errors and fill gaps in the 2002 standards and to supplement them with provisions that address HAVA requirements. In May 2005, TGDC approved a first set of recommended changes and delivered them to EAC. Subsequently, EAC published these changes as proposed voluntary voting system guidelines and requested public comment by September 30, 2005. EAC plans to review and address the comments it receives from the public and its standards and advisory boards during October 2005, and to issue the 2005 Voluntary Voting System Guidelines shortly thereafter, depending on the nature and volume of comments. EAC is proposing that the 2005 voluntary voting system guidelines will become effective 24 months after they are adopted by the EAC, although individual states will be free to adopt the standards at any time during the 24 month period. According to the EAC, the 24 month period is intended to give vendors the time to design and develop systems that comply with the new guidelines; to give testing laboratories the opportunity to develop testing protocols, train laboratory staff, and be prepared to test the systems against the new guidelines; and to allow states time to adopt the standards, adjust their certification and acceptance testing processes, and acquire systems in plenty of time for future election cycles.

Key security and reliability standards of the proposed 2005 guidelines include

- a method for distributing voting system software,
- protocols for generating and distributing software reference data for the NIST repository of certified voting system software,
- a method for validating the proper setup of voting systems,
- controls for the use of wireless communications by voting systems, and
- optional specifications for a voter-verified paper audit trail.

However, NIST reported that several of the topics listed in the proposed guidelines (including software distribution, validation of system setup, and wireless communications) will not be fully addressed in the 2005 update, and will need to be updated in a future version of the guidelines. Furthermore, key security and reliability improvements to the existing standards (including guidance for the security of COTS software; ensuring the correctness of software, testing, and documentation for system security; enhancements to the precision and testability of the standards; and the usability of error messages) have been deferred until the subsequent set of guidelines is developed. EAC officials acknowledged that these changes will not be made in the initial set of guidelines, and reiterated that they are focusing on what can be done in time to meet the HAVA-mandated delivery date for the initial set of guidelines.

Testing. EAC and NIST have initiatives under way to improve voting system testing, including efforts to evaluate and accredit independent testing laboratories (which test voting systems against the national standards) and efforts to define both an interim process and a long-term program for voting system certification.

- NIST is in the process of establishing plans and procedures to conduct an evaluation of independent, nonfederal laboratories through its National Voluntary Laboratory Accreditation Program. NIST solicited feedback from interested laboratories concerning its accreditation program, drafted a handbook that documents the accreditation process, and accepted applications from its first cadre of candidate laboratories through August 2005. The evaluation of candidate laboratories is planned to begin in fall 2005. Once this evaluation is completed, NIST plans to submit for EAC accreditation a proposed list of laboratories to carry out the testing of voting systems. In light of the time required to publicize the accreditation process and requirements and to evaluate the first set of candidates, NIST officials estimated that they would recommend laboratories for accreditation in late 2006 or early 2007. Laboratories that are currently accredited by the National Association of State Election Directors can continue to operate as independent testing authorities until June 2008, but are expected to complete NIST's new accreditation program by that time. In addition, EAC officials stated that they are in the process of developing plans and procedures with NIST and the independent testing authorities to upgrade existing accreditations to address the 2005 voting system standards, when these standards are approved.

- EAC is working to establish a program to certify, decertify, and recertify voting systems. With the assistance of a consulting firm, EAC is in the process of defining certification policies and procedures, both for systems undergoing testing with existing federal voluntary voting system standards and for those that will be tested against EAC's voluntary voting system guidelines. EAC officials expect to define the scope and framework for the certification process and to begin to accept vendor registrations during fall 2005. It also expects to begin accepting applications for certification of voting systems by January 2006. EAC has not yet determined when it will have a national program for voting system certification in place.

Management support. To address its responsibilities related to providing election management support to state and local jurisdictions, EAC and NIST have been working to establish a software library and to act as a clearinghouse for information on both problems and recommended practices involving elections and systems.

- In anticipation of the 2004 elections, EAC and NIST established a software library for voting systems within NIST's National Software Reference Library that allows state and local governments to verify that their voting system software is the certified version (based on testing by independent testing laboratories) and to manage the configuration of that software for their systems. The library was established before the 2004 general election with software from approximately a half dozen major voting system vendors. NIST derived digital signatures for the software and published them on the library's public Web site for states and local jurisdictions to compare with the signatures of software used by their systems.

- In January 2005, TGDC requested that NIST define a process and specification for sharing information among jurisdictions regarding nonconformities, problems, and vulnerabilities in voting systems, to specifically address the security and reliability of those systems. Such information could be used to alert state and local election officials to known problems with their systems and to develop additional recommended practices for their use. TGDC designated this task as a third-tier priority and has deferred working on it until after the publication of the 2005 voting system standards. In addition, EAC surveyed state and local election officials to identify problems they encountered during the 2004 election. However, election officials often interpreted the survey questions differently, so not all of the information

resulting from this survey was complete or usable. EAC plans to enhance its survey activities in the future.

- EAC is charged by HAVA with conducting periodic studies of election administration issues with the goal of providing the most accurate, secure, and expeditious system for voting and tabulating election results.[87] Toward this end, EAC compiled the experiences of a select group of elections experts into a tool kit to help states and local jurisdictions prepare for the 2004 general election.[88] It was published on EAC's Web site in August 2004 and publicized to state and local jurisdictions before the election. The tool kit provides recommendations for methods to manage and operate voting systems to help ensure accurate and secure election results and includes general practices for all voting systems and environments, as well as controls for specific types of voting equipment. Since developing the tool kit, EAC has included additional best practices proposed by TGDC and NIST in the appendixes of its draft voting system guidelines. These practices recommend that election officials establish procedures for their jurisdictions to ensure, among other things, that voting systems are physically secured against tampering and intentional damage, cryptographic keys for wireless encryption are actively managed, actions taken when using wireless communication are logged, and the authenticity of certified software is confirmed using the National Software Reference Library. EAC plans to update the practices in the voting system guidelines and to compile a broader framework of guidance for election administration and management practices that incorporates the best practices tool kit and further promotes security and reliability for voting systems. EAC has begun working with the National Association of State Elections Directors to establish a working group to develop additional guidelines and procedures for election management and operations and has identified the personnel who will support this effort. This fall, EAC expects the working group to develop a comprehensive outline for the election management guidelines document and to prioritize the topics to be developed for the initial version scheduled to be released in December 2006. A final report is expected in December 2007.

[87]Help America Vote Act of 2002, Section 241.

[88]EAC, *Best Practices Tool Kit* (July 2004), http://www.eac.gov/bp/index1.asp.

Tasks and Time Frames for Completing Federal Initiatives Are Not Fully Defined

While EAC has begun several important initiatives to improve the security and reliability of voting systems, more remains to be done on these initiatives, and specific tasks and time frames for performing them are not fully defined.

Standards. EAC recognizes that its planned 2005 update to the standards does not fully address known weaknesses. EAC and NIST are developing an outline for the next iteration of the guidelines, but no date has been set for NIST to deliver the next guidelines draft to TGDC. This rewrite is expected to extensively change the existing standards and include, among other features, quality management for system development, more testable standards, and specifications for ballot formats. However, neither TGDC nor NIST has defined specific tasks, measurable outcomes, milestones, or resource needs for addressing the next draft of standards. Consequently, the time frame for states and local jurisdictions to implement the security and reliability improvements associated with the next version of the standards is unknown. The undefined time frame for completing the standards is likely to cause concern for states required to comply with the federal standards by statute, administrative rule, or condition of HAVA payments, and will further delay the adoption of widely acknowledged capabilities needed for secure and reliable systems.

Voting system certification. While EAC is working to define the scope of a system certification process, much remains to be done before such a process is put in place. Specifically, EAC still needs to establish policies, criteria, and procedures to govern certification reviews and decisions for existing standards, as well as the proposed 2005 standards. However, the specific steps and time frames for EAC to execute each stage of its certification responsibilities have not yet been decided. Until EAC establishes a comprehensive system certification program, its processes may be inconsistent or insufficiently rigorous to ensure that all certified systems meet applicable standards.

Software library. NIST established a software reference library for voting systems, but the usefulness of this library is questionable. The initial set of voting system software deposited into the library was not comprehensive, no additional voting system software has been submitted to the reference library since the 2004 general election, and neither EAC nor NIST has identified specific actions to encourage participation from states, local jurisdictions, vendors, or independent testing authorities for the 2006 federal election cycle. Additionally, state and local jurisdictions require specialized tools and technical support to verify that reference library

software signatures match those of their own software versions, but no consolidated and easily accessible list of sources for these tools and services is currently available to state and local jurisdictions. Further, NIST did not keep statistics on the extent to which state and local jurisdictions used the library during the 2004 election cycle to verify installation of certified software by their vendors, and thus, it could not determine whether its service was meeting state and local needs. Without the continuous incorporation of certified software into the library and processes that can be effectively implemented by state and local governments, these entities are likely to face difficulty in ensuring that their tested and operational voting systems are the same as those that were certified. Further, without a mechanism for determining how the library is being used and how it can be improved, the potential benefits of the library may be greatly diminished.

Clearinghouse for information on problems and leading practices. To fulfill its role as a clearinghouse for information on voting system problems, EAC continues to explore issues of data collection for problems with voting systems through enhancing its survey instrument to collect problem information from election officials and working with NIST to determine how to share this information. However, neither EAC nor NIST has defined specific tasks or time lines for establishing procedures for sharing problems or a repository for collecting them. The continued absence of a national clearinghouse for voting system problems means that segments of the election community may continue to acquire and operate their systems without the benefit of critical information learned by others regarding the security and reliability of those systems. Regarding its efforts to develop broad guidance on election administration practices, EAC has initial plans for moving forward, but lacks a process and schedule for compiling and disseminating this information on a regular basis. Until EAC puts such a process in place, there is a risk that the guidance it provides may become outdated and of little value to election officials.

Although EAC initiatives are expected to eventually provide more secure and reliable systems and more rigorous and consistent quality assurance processes for the states and jurisdictions that choose to use them, how, when, and to what degree this will be accomplished is not clear. Specific steps have not been identified to implement some of the initiatives in time to affect the 2006 general election, and others are not expected to be completed until after the 2006 election. This situation is due, in part, to delays in the appointment of EAC commissioners and in funding the

commission. As a result, it is unclear when the results of these initiatives will be available to assist state and local election authorities.

Nongovernmental Initiatives Are Intended to Improve Voting System Security and Reliability

In addition to federal initiatives, initiatives by various nongovernmental organizations nationwide have been established to address the security and reliability of voting systems. Professional organizations, academic institutions, and citizen advocacy groups have initiatives that affect several areas of the voting system life cycle, particularly product development, acquisition, standards, and management. Selected initiatives include (1) developing open designs for voting system products; (2) identifying issues and key questions to be considered by consumers of electronic voting systems; (3) defining international standards; and (4) supporting more effective management, including collecting, cataloging, and analyzing problems experienced during elections. Table 3 summarizes key initiatives.

Table 3: Nongovernmental Initiatives to Improve Voting System Security and Reliability

Initiative	Organization	Product or activity	Status
Product development			
Prototype for an open-source electronic voting application	Open Voting Consortium	Developed a prototype for an open-source electronic voting application that uses commercial hardware and operating system components and provides (1) an electronic voting machine that prints a paper ballot, (2) a ballot verification station that scans the paper ballot and lets a voter hear the selections, and (3) an application to tally the paper ballots.	Continuing to add functionality to prototype. No specific timetable.
A Modular Voting Architecture	Caltech/MIT Voting Technology Project	Proposed an approach for building additional security features into electronic voting systems through an alternative voting system architecture.	Completed August 2001. Available for implementation.
Acquisition			
A Framework for Understanding Electronic Voting	National Academy of Sciences' Computer Science and Telecommunications Board	Defining questions to help policy makers, election officials, and the interested public understand the technology, social, and operational issues relevant to electronic voting, including security issues.	Publication expected in fall 2005.
Relative performance of voting system classes	Brennan Center for Justice	Started an independent assessment of electronic voting system security and plans to develop a report describing the relative performance of each class of voting systems.	To be completed in fall 2005.

(Continued From Previous Page)

Initiative	Organization	Product or activity	Status
Standards			
Project 1583 on Voting Equipment Standards	Institute of Electrical and Electronics Engineers	Developing a standard for voting equipment requirements and evaluation methods, including security and reliability characteristics.	Project 1583 members in recess. No current plans to resume this project's activities.
Project 1622 on Voting Equipment Electronic Data Interchange	Institute of Electrical and Electronics Engineers	Developing data formats to be used by voting system components for exchange of electronic data, including data related to secure and reliable system operations.	Project 1622 officials are working to endorse a draft standard. No specific timetable.
Election Markup Language	Organization for the Advancement of Structured Information Standards	Defined process and data requirements that include security considerations for authentication, privacy/confidentiality, and integrity.	Officials are seeking approval for this markup language as an international standard from the International Organization for Standardization. No specific timetable.
Testing			
Voting System Performance Rating	Voting System Performance Rating	Developing evaluation and performance assessment tests for use in rating the performance of voting systems in subject areas such as privacy, transparency, and ballot verifiability.	Working groups are being organized and members plan to draft, publish, and distribute a range of documents in each of the relevant subject areas over the next 2 years.
Management			
Professional Education Program	The Election Center	Created a professional education program designed to provide training and certification to election officials and vendors.	Continuing to expand the curriculum. No specific timetable.
Election Incident Reporting System	Verified Voting	Operating the Election Incident Reporting System, a Web-based system to collect and disseminate information about local voting systems and election irregularities.	Plans to operate through future elections. No specific timetable for supporting activities.
Information clearinghouse	VotersUnite!	Operating a repository of news and events and a newsletter service to share information among advocacy groups and jurisdictions on a wide range of electronic voting problems and issues.	Ongoing postings. Continuation uncertain due to limited resources.
A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections	Johns Hopkins University	Created a federally funded center that is to conduct (1) research into the technological issues facing electronic voting, (2) education efforts, aimed at higher education, focusing on voting technology issues, and (3) outreach to stakeholders in the election administration process, including vendors, election officials, and community groups.	Plans to conduct activities over 5 years.

Source: GAO summary of data provided by organizations listed above.

Conclusions

Electronic voting systems hold promise for improving the efficiency, accuracy, and accessibility of the elections process, and many are in use across the country today. The American public needs to feel confident using these systems—namely, that the systems are secure enough and reliable enough to trust with their votes. However, this is not always the case. Numerous recent studies and reports have highlighted problems with the security and reliability of electronic voting systems. While these reports often focused on problems with specific systems or jurisdictions, the concerns they raise have the potential to affect election outcomes. The numerous examples of systems with poor security controls point to a situation in which vendors may not be uniformly building security and reliability into their voting systems, and election officials may not always rigorously ensure the security and reliability of their systems when they acquire, test, operate, and manage them.

These concerns have led to action. Multiple organizations have compiled recommended practices for vendors and election officials to use to improve the security and reliability of voting systems, and EAC has initiated activities to improve voluntary voting system standards, system testing programs, and management support to state and local election authorities. However, important initiatives are unlikely to affect the 2006 elections due, at least in part, to delays in the appointment of EAC commissioners and in funding the commission. Specifically, key security-related improvements to voting system standards will not be completed in time, improvements to the national system certification program are not yet in place, and efforts to provide management support to state and local jurisdictions through a software library and information sharing on problems and recommended practices remain incomplete. Further, EAC has not consistently defined plans, processes, and time frames for completing these activities, and as a result, it is unclear when their results will be available to assist state and local election officials. Until these efforts are completed, there is a risk that many state and local jurisdictions will rely on voting systems that were not developed, acquired, tested, operated, or managed in accordance with rigorous security and reliability standards—potentially affecting the reliability of future elections and voter confidence in the accuracy of the vote count.

Recommendations for Executive Action

To improve the potential for benefits to states and local election jurisdictions, we recommend that the Election Assistance Commission take the following five actions:

1. Collaborate with NIST and the Technical Guidelines Development Committee to define specific tasks, measurable outcomes, milestones, and resource needs required to improve the voting system standards that affect security and reliability of voting systems.

2. Expeditiously establish documented policies, criteria, and procedures for certifying voting systems that will be in effect until the national laboratory accreditation program for voting systems becomes fully operational, and define tasks and time frames for achieving the full operational capability of the national voting system certification program.

3. Improve management support to state and local election officials by collaborating with NIST to establish a process for continuously updating the National Software Reference Library for voting system software; take effective action to promote use of the library by state and local governments; identify and disseminate information on resources to assist state and local governments with using the library; and assess use of the library by states and local jurisdictions for the purpose of improving library services.

4. Improve management support to state and local election officials by collaborating with TGDC and NIST to develop a process and associated time frames for sharing information on the problems and vulnerabilities of voting systems.

5. Improve management support to state and local election officials by establishing a process and schedule for periodically compiling and disseminating recommended practices related to security and reliability management throughout the system life cycle (including the recommended practices identified in this report) and ensuring that this process uses information on the problems and vulnerabilities of voting systems.

Agency Comments and Our Evaluation

EAC and NIST provided written comments on a draft of this report (see apps. V and VI). EAC commissioners agreed with our recommendations and stated that actions on each are either under way or intended. NIST's director agreed with the report's conclusions that specific tasks, processes, and time frames must be established to improve the national voting systems standards, testing capabilities, and management support available to state and local election officials.

In addition to its comments on our recommendations, EAC commissioners expressed three concerns with our use of reports produced by others to identify issues with the security and reliability of electronic voting systems. First, they noted that the draft lacked citations linking security problems and vulnerabilities to the reports in the bibliography and lacked context when referring to experts. We have since provided citations and context, where applicable. Second, commissioners expressed concern that the report portrays voting system problems as systemic, but does not provide context for evaluating the extent of the problems—that is, how frequently these issues arise or whether the problems occur in a large percentage of electronic voting systems or jurisdictions. We do not agree that we portray the problems as systemic. Our report states that many of the issues involved specific voting system makes and models or circumstances in the elections of specific jurisdictions, and that there is a lack of consensus on the pervasiveness of the concerns. This is due in part to a lack of comprehensive information on what system makes and models are used in jurisdictions throughout the country. Nonetheless, the numerous examples of systems with poor security controls point to a situation in which vendors may not be uniformly building security and reliability into their voting systems, and election officials may not always rigorously ensure the security and reliability of their systems when they acquire, test, operate, and manage them. Third, commissioners expressed concern that our report relies on reports produced by others without substantiation of the claims made in those reports, and provides specific examples that they felt should be verified with election officials. While our methodology focused on identifying and grouping problems and vulnerabilities identified in issued reports and studies, where appropriate and feasible, we sought additional context, clarification, and corroboration from the authors, election officials, and security experts. In one of the specific examples offered by EAC, we understand that the Florida demonstration may not have offered an accurate assessment of the system's vulnerabilities to outsiders, but it has value in identifying vulnerabilities to knowledgeable insiders. In another example, EAC takes issue that we found no concerns with the security and reliability during the acquisition phase of the voting system life cycle and noted that they learned from state and local officials that a number of voting equipment units have recently been rejected during the acceptance testing phase of the acquisition process demonstrating quality assurance or reliability concerns. We do not question EAC's point, but this issue did not surface in the reports we analyzed and the interviews we held—so we did not include it in our report. This issue, however, shows that there could be security and reliability issues that are not documented in existing reports. Assessing security and reliability issues and

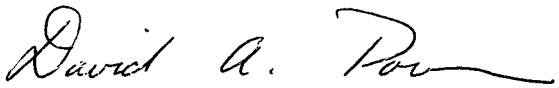
determining their pervasiveness are items that EAC can explore and share in its role as a clearinghouse for information on problems with electronic voting systems.

EAC commissioners also commented that our report focuses exclusively on EAC as the answer to the questions surrounding electronic voting, and stated that EAC is but one participant in the process of ensuring the reliability and security of voting systems. They noted that while EAC, TGDC, and NIST are working to develop a revised set of voting system guidelines (standards), it is the voting system vendors that must design and configure their systems to meet those guidelines and the state and local election officials that must adopt the guidelines and restrict their purchases of voting systems to ones that conform to the guidelines. While we agree that EAC is one of many entities with responsibilities for improving the security and reliability of voting systems, given its leadership role in defining voting system standards, in establishing programs both to accredit laboratories and to certify voting systems, and in acting as a clearinghouse for improvement efforts across the nation, we believe that our focus on EAC is appropriate and addresses the objective of our requesters regarding the actions that federal agencies have taken.

EAC and NIST officials also provided detailed technical corrections, which we incorporated throughout the report as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the report date. At that time, we will send copies of this report to the Chairman and Ranking Member of the Committee on House Administration and to the Chairman and Ranking Member of the Senate Committee on Rules and Administration. We are also sending copies to the Commissioners and Executive Director of the Election Assistance Commission, the Secretary of Commerce, the Director of the National Institute of Standards and Technology, and other interested parties. In addition, the report will be available without charge on GAO's Web site at http://www.gao.gov.

Should you have any questions about matters discussed in this report, please contact Dave Powner at (202) 512-9286 or at pownerd@gao.gov or Randy Hite at (202) 512-3439 or at hiter@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs can be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix VII.



David A. Powner
Director, Information Technology
Management Issues

Randolph C. Hite
Director, Information Technology Architecture
and Systems Issues

List of Congressional Requesters

The Honorable Tom Davis
Chairman
The Honorable Henry A. Waxman
Ranking Minority Member
Committee on Government Reform
House of Representatives

The Honorable Jim Sensenbrenner, Jr.
Chairman
The Honorable John Conyers, Jr.
Ranking Minority Member
Committee on the Judiciary
House of Representatives

The Honorable Sherwood L. Boehlert
Chairman
The Honorable Bart Gordon
Ranking Minority Member
Committee on Science
House of Representatives

The Honorable William Lacy Clay
House of Representatives

The Honorable John B. Larson
House of Representatives

The Honorable Todd Platts
House of Representatives

The Honorable Adam Putnam
House of Representatives

The Honorable Ileana Ros-Lehtinen
House of Representatives

The Honorable Robert C. Scott
House of Representatives

The Honorable Christopher Shays
House of Representatives

The Honorable Michael Turner
House of Representatives

Objectives, Scope, and Methodology

Our objectives were to (1) determine significant security and reliability concerns that have been identified for electronic voting systems; (2) identify recommended practices relevant to the security and reliability of such systems; and (3) describe the actions that federal agencies and other organizations have taken, or plan to take, to improve the security and reliability of electronic voting systems. Our work focused on the security and reliability of optical scanning and direct recording electronic voting systems, which includes equipment for defining ballots, casting and counting ballots, managing groups of interconnected electronic components, and transmitting voting results and administrative information among the locations supporting the voting process.

To determine significant security and reliability concerns and identify recommended practices, we conducted a broad literature search for existing published electronic voting studies. Our search included the use of Internet sources, technical libraries, professional and technical journals, and bibliographic information from articles and documents we obtained. We also collected citations and contacts during interviews with relevant officials and experts. To corroborate and provide context for identified concerns and recommended practices, we interviewed federal officials, election officials, computer and information security experts, industry officials, and citizen advocacy groups. Our interviews also included officials from nongovernmental organizations involved with elections and electronic voting issues, as well as members of our Executive Council on Information Management and Technology. In addition, we examined testimony made before pertinent federal bodies and other source material to provide supporting information.

Through our literature search, we identified a number of reports that addressed electronic voting issues. We organized these reports into several content areas, including system security assessments, reliability issues, general security issues, practices and recommendations, and statistical analyses. To identify the most relevant sources for our work, we then selected those reports that best met selection criteria that we developed. The selection criteria included the extent to which the report specifically addressed the security and reliability of electronic voting systems and recommended practices relevant to these systems; whether original data analysis was conducted; author knowledge and experience; endorsements by pertinent government organizations (which were often sponsors of reports); and the authenticity of available copies of the report. We were interested in targeting the more recent literature, but we included earlier reports that were deemed particularly relevant to the objectives of our

work.[1] To assist in our assessment of the reliability of each report's findings, we also conducted reviews of a report's methodology, including its limitations, data sources, and conclusions. We also obtained permission to use and report on any documents that were marked as confidential or otherwise sensitive.[2] The final lists of the selected literature we relied on for our work are shown in the bibliography.[3] Some reports were not selected. For the most part, these reports did not directly focus on our work objectives, and the selected reports presented a more thorough treatment of the issues related to our work.

From the selected literature and corroborating interviews, we extracted and summarized findings to create a list of security and reliability concerns for electronic voting systems. We also identified and summarized recommended practices for improving the security and reliability of electronic voting systems. Additionally, we included generally recommended practices issued by the federal government and other organizations that promote security and reliability for information systems engineering and management. We examined these general practices to confirm their applicability to the voting environment. However, our review of the recommended practices did not include validating the quality or assessing the effectiveness of the practices, or the extent to which the practices have been implemented by states or local jurisdictions. Finally, using a systems life cycle framework, we organized our list of concerns and recommended practices according to the activities in the voting system life cycle model that we developed.[4]

To describe the actions that federal agencies and other organizations have taken, or plan to take, to improve the security and reliability of electronic voting systems, we reviewed the Help America Vote Act to determine

[1]For example, a 1988 National Bureau of Standards report on the accuracy, integrity, and security of computerized vote-tallying is still considered relevant.

[2]The documents that were marked as sensitive have been made available to the public, and thus the markings are no longer applicable.

[3]Reports and studies that include concerns about the security and reliability of electronic voting systems are listed separately from those that identify recommended practices. However, there is some overlap between the lists in that some of the reports that identified concerns also recommended measures to address these concerns.

[4]This model identifies key phases in a voting system's life cycle, including development, acquisition, and operations as well as cross-cutting activities involving use of standards, testing, and management.

federal responsibilities and requirements for improving the security and reliability of electronic voting systems. We attended public meetings of the Election Assistance Commission, the National Institute of Standards and Technology, and the Technical Guidelines Development Committee; conducted interviews with officials from these organizations and others; and obtained and analyzed supporting documents, including the Voluntary Voting System Guidelines and the resolutions of the Technical Guidelines Development Committee. We evaluated the resolutions to identify those relevant to security and reliability and identified the committee's priorities and plans for implementing the resolutions. Additionally, we identified activities being performed by nongovernmental organizations to improve the security and reliability of electronic voting systems through a broad literature search and interviews with electronic voting experts. These organizations, including citizen advocacy groups as well as academic and standards bodies, were selected based upon the degree to which their initiative's goal addressed our objective (to improve the security and reliability of electronic voting systems), the demonstrated progress toward achieving the goal, the existence of plans for specific products or activities, and willingness to discuss and confirm each of these areas with us. We conducted interviews with members of the nongovernmental organizations and analyzed supporting documentation provided by them or available on their Web sites. We did not evaluate the quality or effectiveness of these nongovernmental initiatives.

We conducted our work at the Election Assistance Commission, the National Institute of Standards and Technology, the National Academies of Science, and several nongovernmental organizations in the Washington, D.C., area. Our work was performed from January through August 2005 in accordance with generally accepted government auditing standards.

Selected Recommended Practices for Voting System Security and Reliability

Multiple organizations have issued collections of recommended practices for establishing secure and reliable electronic voting systems. For example, the Election Assistance Commission's Best Practices Tool Kit is a central document for guidance on this topic. Developed under HAVA for use by state and local election officials, this Web-based resource presents guidance compiled from experienced representatives of the election community, with links to Web-based references from a variety of organizations where additional recommended practices are documented. The tool kit references practices and studies from other organizations, including the National Institute of Standards and Technology, the Brennan Center for Justice at New York University, the Leadership Conference on Civil Rights, the Caltech/MIT Voting Technology Project, and the Election Center. Other organizations have also issued their own sets of recommended practices. Many of the reports and studies that we reviewed to identify concerns with electronic voting systems also offered recommendations for mitigating the weaknesses they found. The descriptions below summarize the aspects of this guidance pertaining to the security and reliability of voting systems.

Election Assistance Commission: Best Practices Tool Kit. The Help America Vote Act (HAVA) tasked the EAC with promoting, among other things, accurate, convenient, and efficient methods of voting and election administration in a variety of areas, including voting technology, ballot design, and poll worker training. As part of its efforts to address this requirement, EAC assembled a team of elections officials for a 2-day working session in mid-2004 to create a "Best Practices Tool Kit." The tool kit is a compendium of practices recommended by elections experts, including state and local jurisdictions. The immediate goal of the tool kit was to help local election administrators in their management of the 2004 elections. The practices and recommendations in the tool kit address the life cycle activities of acquisition, operations, testing, and management. The tool kit also includes practices that are specific to ensuring the security and reliability of different types of electronic voting systems in the areas of testing, operations, and management. Example practices from the tool kit are provided in the following tables: table 4 identifies practices that pertain to all types of voting systems, table 5 identifies practices that pertain to optical scan voting systems, and table 6 identifies practices that pertain to direct recording electronic (DRE) voting systems.

Table 4: EAC Security and Reliability Practices for All Types of Voting Systems

Life cycle activity	Example practice
Acquisition	• Develop a budget and procurement plan; make sure the procurement process is open to public scrutiny and abides by state and county or municipal guidelines. • Before purchasing equipment or before implementation, you may find it helpful to consult the National Institute of Standards and Technology (NIST) analysis, "Recommended IT Security Product Life Cycle Product Planning." The analysis provides a road map for planning, purchasing, using, maintaining, and transitioning to electronic voting equipment, with a particular focus on the security issues related to electronic voting equipment.
Operations	• Draft and implement well-organized procedures that identify the chain of custody for every instance when the ballots and/or voting equipment changes hands. • Separate staff duties for each test you conduct, and require staff signatures to ensure each procedure has been completed and appropriately documented. • If you must deliver election equipment or supplies to the polling place before election day, seal equipment, supply boxes, and each sensitive item in the box so you will know if tampering has occurred. • Restrict access to election office both before and after election. At the polling place, provide badges to poll workers and pollwatchers. At your election headquarters, require staff and visitors to sign in, sign out, and wear badges. • Conduct a postelection audit of all electronic systems. • Verify that the number of ballots cast matches the number of voters who signed each precinct's roster. • Develop administrative procedures (or implement those procedures developed by state officials) to audit the accuracy of your election results. • If you are using a modem to transmit your unofficial results, use a phone line—not a wireless connection—and ensure the modem encrypts the information.
Testing	• To reduce the risk of raising public concerns, conduct pre-testing before conducting a public test to ensure that the machines are working properly. • Test every piece of voting equipment before deployment, using the ballot styles for that election. Invite the public and media to a public test of the system.
Management	• Focus early on poll worker recruitment and training; poll workers should practice each important component of the election process, especially using the voting equipment. • Include chain of custody instructions in poll worker training. • Prepare back-up and emergency plans; conduct a risk analysis of the election process and develop a plan for dealing with worst-case scenarios. • If introducing a new voting system, conduct voter and media outreach. Develop brochures; set up self-help voting laboratories or kiosks at city halls, libraries, etc.; loan demonstration units to community organizations; prepare materials for media outreach and conduct pre-election briefings. • Request that your vendor submits its certified software to the National Software Reference Library (NSRL) at the National Institute of Standards and Technology (NIST). • Have your vendor supply you with a copy of its letter to NIST and the state election office confirming receipt of the version of the software that you are using. • You may wish to contact NIST to inquire and to confirm that the version of your vendor's software matches the certified version of the software on file with NIST. • Obtain documentation from your voting system vendor regarding the national and/or state testing and certification that the system has been through. Double check by contacting the state election office to substantiate that your system as installed has been certified.

Source: GAO summary and categorization of EAC report.

Table 5: EAC Security and Reliability Practices for Optical Scan Voting Systems

Life cycle activity	Example practice
Operations	• Establish security procedures for printing and shipping of ballots. • For in-precinct optical scan equipment, check to see that the internal ballot box is empty at beginning of the day. Poll workers should keep keys for machine and ballot box in a secure location. • Have two poll workers transport results.
Testing	• Test the calibration of every scanner before the election. • Conduct printing tests and quality control tests.
Management	• If using in-precinct counting system, provide poll workers with a script for assisting the voter without compromising voter privacy. • Provide poll worker training on ballot and equipment storage requirements and security measures. • Develop a troubleshooting plan. Define the response time—know how long it will take to get a troubleshooter to the polling place. • Establish procedures for handling a machine failure, such as roving technicians, a technical help desk, and technical back-up support. • Establish procedures for when security measures are not followed, such as when materials come back unsealed or unsigned.

Source: GAO summary and categorization of EAC report.

Table 6: EAC Security and Reliability Practices for Direct Recording Electronic Voting Systems

Life cycle activity	Example practice
Operations	• Track overvotes and undervotes. Develop election day procedures to help determine the nature and cause of undervotes and blank votes to determine whether they are genuine undervotes or the result of voter confusion. • Require poll workers to keep a log of election day events and problems, including voter complaints, that will help you to recreate the events of the day. • Keep a maintenance log for all voting system equipment. This log should track who has had access to the machines. • Develop chain of custody for memory cards and machines. • Control access to the voter "smart cards." • Develop rules for access to any sensitive equipment. • Check the machine's public vote counter to verify that the number of voters who signed in matches the number of the public counter. Account for any discrepancies.
Testing	• Conduct, at a minimum, both acceptance testing and logic and accuracy testing on each system. Logic and accuracy testing should include "incremental testing." • Conduct system diagnostics on every machine for every election before you conduct logic and accuracy testing. • Conduct postelection logic and accuracy testing of machines.
Management	• Create a poll worker position that is dedicated to machine setup, shutdown, and troubleshooting. Provide supplemental training on equipment; supplement pay for extra training. • Establish written procedures for handling election day equipment failure. • Conduct a risk analysis—where are you most vulnerable to problems? At what points are the system—both the administrative system and the machines—most likely to break down? For example, is there an indispensable person? If so, develop a plan for dealing with his/her absence. Develop contingency plans, such as off-site storage of all software and data. • Ensure that all software, including patches, is certified.

Source: GAO summary and categorization of EAC report.

National Bureau of Standards: Accuracy, Integrity, and Security in Computerized Vote-Tallying (NBS SP 500-158). In August 1988, the National Bureau of Standards (the prior name for NIST) issued a report authored by a well-known elections expert.[1] The report is referenced by EAC's tool kit. It makes recommendations regarding the life cycle activities of product development, operations, testing, and management that are intended for state and local elections officials. The recommendations are largely related to implementation of administrative controls and operational procedures, although the recommendations related to system design are more specific. Example recommendations from the report are given in table 7.

[1]Roy Saltman, *NBS SP 500-158: Accuracy, Integrity, and Security in Computerized Vote-Tallying* (Gaithersburg, Md.: National Bureau of Standards, August 1988). Despite the age of this document, it is still considered relevant and useful.

Table 7: NIST Security and Reliability Practices for Electronic Voting Systems

Life cycle activity	Example practice
Product development	• A computerized vote count should be able to be reproduced on a recount with no more than a change in one vote for each ballot position in ballot quantities of up to 100,000 when machine-generated ballots are used. • Each DRE machine should be designed so as to take a positive action indicating a "no vote" for every choice that the voter fails to take.
Operations	• It is strongly recommended that certified vote-tallying software not be allowed to run on a multiprogrammed general-purpose computer on which uncertified support software or applications also are being run. • Access (i.e., security) controls must be in place during preparations for voting, voting itself, and vote-tallying. These controls concern access to sites, areas, facilities, equipment, documents, files, and data. • Application internal controls for DRE systems should be in place that cover matching machine use with voter totals, vote reconciliations on each machine, recounting of voter-choice sets, and postelection checkout of machines.
Standards	• Each state should consider the adoption of the Federal Election Commission clearinghouse specifications.
Testing	• All vote-tallying software, and all software used with it, should be reviewed for integrity, that is, for the ability to carry out its asserted function and to contain no hidden code. • Vote-tallying software should be tested for logical correctness. • DRE data entry hardware should be certified for logical correctness by examination of the logic design and by testing under a large variety of different conditions. • Sufficient pre-election testing should be done so that errors in software specialization or in implementation of logical rules, if any, will become obvious.
Management	• Expertise in internal control (which includes computer security) should be added to the personnel complement in election administration in order to assure implementation of applicable concepts.

Source: GAO summary and categorization of NIST report.

Brennan Center for Justice: Recommendations of the Brennan Center for Justice and the Leadership Conference on Civil Rights for Improving Reliability of Direct Recording Electronic Voting Systems. In 2004, the Brennan Center for Justice at New York University and the Leadership Conference on Civil Rights assembled a group of election and technology experts to independently assess the security of DRE systems and to develop recommendations for improving DRE reliability. The group issued its recommendations in June 2004.[2] The recommendations are high-level

[2]The Brennan Center for Justice, *Recommendations of the Brennan Center for Justice and the Leadership Conference on Civil Rights for Improving Reliability of Direct Recording Electronic Voting Systems*, (Washington, D.C.: June 2004), http://www.votingtechnology.org/docs/FinalRecommendations.doc?PHPSESSID=05cc9fce915ccfdaa7aa2a154b5b7a6e (downloaded Oct. 1, 2004).

policy recommendations and broad procedural statements rather than low-level practices, and are focused primarily in the life cycle area of management, with one recommendation each in the areas of operations and testing. They were intended for use by elections officials in jurisdictions planning to use DREs in the 2004 elections. The EAC cited this report in its tool kit. Example practices from the report are listed in table 8.

Table 8: Brennan Center Example Security and Reliability Practices for Direct Recording Electronic Voting Systems

Life cycle activity	Example practice
Operations	• Elections officials should establish standard procedures for regular reviews of audit facilities and operating logs for voting terminals and canvassing systems to verify correct operation and uncover any evidence of potential security breaches.
Testing	• Elections officials should develop procedures for random parallel testing of the voting systems in use to detect malicious code or bugs in the software.
Management	• Elections officials should hire a well-qualified, independent security team to examine the potential for operational failures of and malicious attacks against the jurisdiction's DRE voting system. • The assessment performed by the independent security team should cover at least the following areas of concern: hardware design, hardware/firmware configuration, software design, software configuration, election procedures, and physical security. • Election officials should implement the critical recommendations of the independent expert security team and demonstrate to experts and voters alike that the recommendations have been implemented. • Election officials should provide a thorough training program for all election officials and workers to ensure that security procedures, including those recommended by the independent expert security team, are followed even in the face of election day exigencies. • All jurisdictions should prepare and follow standardized procedures for response to alleged or actual security incidents that include standardized reporting and publication. • Election officials should have in place a permanent independent technology panel, including both experts in voting systems and computer security and citizens representing the diverse constituencies involved in election oversight, to serve as a public monitor over the entire process outlined above and to perform a postelection security and performance assessment.

Source: GAO summary and categorization of Brennan Center report.

Election Center: Election Preparation Checklists. In May 2004, the Election Center issued a series of five checklists designed to help state and local election officials prepare for the November 2004 elections.[3] The checklists include specific guidance in the areas of polling place accessibility, security of paper ballots, polling place preparations, voting systems, and procedures for recounts. The EAC tool kit references the

[3]Election Center, *Accessibility Preparations Checklist* (Houston, Tex.: May 2004); *Checklist for Ballot Security* (Houston, Tex.: May 2004); *Checklist for Polling Place Preparations* (Houston, Tex.: May 2004); *Recount Procedures* (Houston, Tex.: May 2004); and *Voting Systems Checklist* (Houston, Tex.: May 2004).

checklists as a group, and specifically notes the accessibility and voting systems checklists. Taken together, the checklists include recommendations in the life cycle areas of operations, testing, and management. Example recommendations are listed in table 9.

Table 9: Election Center Security and Reliability Practices for Elections

Life cycle activity	Example practice
Operations	Ballot security: • Are the polling place scanners/tabulators zeroed and sealed, and the seal number recorded? • Are the polling place scanners/tabulators and system software prepared? • Have you done a complete accounting to reconcile all numbers (so that every ballot, used and unused, is accounted for)? Polling place preparations: • Have you prepared a list of duties (in time frame sequence) that need to be accomplished in order to secure polling locations? • Does the facility have sufficient electrical outlets? Voting systems: • Have labels been printed for memory cards/tabulation chips, receipt envelopes, machine tapes, envelopes, etc.? • Have all peripheral voting supplies been packed, proofed, and secured? Recount procedures: • Keep an audit log of equipment programming, including the retention of all nightly backups until after the deadline for recounts has passed. • Make certain all ballot containers are sealed, labeled, and accounted for. • Schedule recount. Establish complete calendar of events. • Open sealed containers only when recount board and observers are present. • If manual count differs from the original results, you may want to have a different recount team validate the results. • Conduct every election as if it will be recounted. Public perception is vital in conducting a recount. Providing information and forms in an organized manner strengthens the perception of the overall integrity of the process.
Testing	Ballot security: • Has logic and accuracy testing been completed? Voting systems: • Has logic and accuracy testing been scheduled? • Has manual logic and accuracy testing been performed on every tabulation chip/memory card in its election-specific machine? Recount procedures: • Keep an audit log of all equipment testing. • Conduct the public test as published. Even if there are no observers, it is important to be able to show that you performed a formal and complete test of the system.

(Continued From Previous Page)

Life cycle activity	Example practice
Management	Polling place preparations: • Have you prepared a poll worker manual? • Have you prepared training materials, including audio-visual materials? Voting systems: • Have pertinent federal laws that affect voting systems been researched for an understanding of requirements? • Have training materials for election workers been prepared and printed? • Have election workers been notified and assigned to training classes? • Are you on the latest, tested, certified version of your voting system software?

Source: GAO summary and categorization of Election Center report.

National Task Force on Election Reform: Election 2004: Review and Recommendations by the Nation's Elections Administrators. In early 2005, the National Task Force on Election Reform within the Election Center began to assemble its report on the 2004 election. The task force was divided into three subcommittees in the areas of voter registration, election technology, and redesigning elections; the recommendations of each subcommittee were combined to produce the final report and recommendations that were issued in May 2005.[4] The recommendations relevant to the security and reliability of electronic voting systems are directed to NIST, the EAC, state governments, and state and local election officials. They address the life cycle activities of acquisition, standards, testing, and management, with one recommendation in the area of operations. Examples of the task force's recommendations relevant to the security and reliability of voting systems are listed in table 10.

[4]National Task Force on Election Reform, *Election 2004: Review and Recommendations by the Nation's Elections Administrators* (Houston, Tex.: Election Center, May 2005).

Table 10: National Task Force on Election Reform Security and Reliability Practices for Voting Systems

Life cycle activity	Example practice
Acquisition	In the area of procurement of equipment, the task force recommends: • That the EAC develop and maintain a library of requests for proposals (RFPs), contracts, and customer complaints as a resource for purchasing jurisdictions. • That states are encouraged to assist in procuring voting equipment for local jurisdictions. • That purchasing jurisdictions carefully and thoroughly document each step of the procurement process. • That the acquisition process require acceptance testing, independent of the vendor, of all equipment and system components (hardware and software) as part of the procurement and contract requirements.
Operations	In the area of Voter Verifiable Paper Audit Trail, the task force recommends: • That states develop procedures to safeguard and retain any paper record receipt in the polling place to preserve secrecy of the voted ballot.
Standards	In the area of procurement of equipment, the task force recommends: • That states adopt the voluntary voting system standards issued by the Federal Election Commission and the voluntary voting system guidelines issued by the U.S. Election Assistance Commission. In the area of Voter Verifiable Paper Audit Trail, the task force recommends: • That guidelines be developed by the National Institute of Standards and Technology, through the EAC, for a scientifically sound, independently verifiable audit trail for DRE voting systems and that such guidelines not be restricted to contemporaneous paper replica but also include guidelines for electronic, audio, video, or other media to provide verification of the integrity of recording and tabulating votes. • That, for DRE voting systems, guidelines be developed by NIST, through the EAC, for the contemporaneous recording of each ballot record, on a secure medium, to provide a redundant record of votes.
Testing	In the area of logic and accuracy testing, the task force recommends: • That state and local election administrators develop and make available to the public written documentation describing their logic and accuracy testing procedures. These procedures should be standardized throughout the state for each voting system. • That the date and location of logic and accuracy testing be publicized through media releases and public Web pages. • That NIST provide testing standards and procedures by equipment type for use by local and state election administrators in conducting logic and accuracy testing. • That local election administrators develop internal staffing procedures to control, manage, and document the logic and accuracy testing of their jurisdiction's voting equipment.
Management	In the area of poll worker recruitment and retention, the task force recommends: • That state and local jurisdictions implement supplemental training and recognition programs for poll workers. In the area of procurement of equipment, the task force recommends: • That election officials develop clear, uniform, and nondiscriminatory policies for determining the number of voting devices per polling site.

Source: GAO summary and categorization of National Task Force on Election Reform report.

Caltech/MIT Voting Technology Project: Voting—What Is, What Could Be. The Caltech/MIT Voting Technology Project issued its first report in July 2001.[5] Its recommendations are intended for all U.S. officials with a role in the voting process. The report provides an overview of the problems with election recounts and system failure that were exposed during the 2000 presidential election controversy; makes recommendations related to voting equipment, voter registration, polling place operations, absentee and early voting, ballot security, and the cost and financing of elections; and makes recommendations for the future of the voting environment, such as proposing a new voting system architecture, calling on the federal government to establish a National Elections Research Laboratory, and calling for the greater national collection and reporting of election administration data. The recommendations in the report are primarily high-level policy proposals and apply to each area of the voting system life cycle, including product development, acquisition, operations, standards, testing, and management activities. Some example recommendations from the report are listed in table 11.

[5]Caltech/MIT Voting Technology Project, *Voting—What Is, What Could Be* (July 2001). http://www.vote.caltech.edu/media/documents/july01/July01_VTP_Voting_Report_Entire.pdf (downloaded Oct. 1, 2004).

Table 11: Caltech/MIT Security and Reliability Practices for Voting Systems

Life cycle activity	Example practice
Product development	• Move away from complex, monolithic machines, to systems using a simple electronic vote-recording device that is separate from other parts of the system. • Make source code for all vote recording and vote counting processes open source and source code for the user interface proprietary. • Design equipment that logs all events (votes, maintenance, etc.) that occur on the machine.
Acquisition	• Replace types of equipment that show high rates of uncounted, unmarked, and spoiled ballots with optically scanned paper ballots that are scanned at the polling place by the voter, or any electronic technology proven in field tests.
Operations	• Conduct audits of votes and equipment, even without a recount. • Election administrators should measure the performance of individual polling places in the areas of arrival process, authorization to vote, voter education, and staffing practices and adopt management principles to improve service.
Standards	• The federal government should create and operate a National Election Standards Commission to use historically proven methods to develop standards. • Within the existing standards framework: Include real voters in testing process Test equipment as it is set up and used at the polling place Require that all noninterface software be open source Retest systems after field use Perform random system audits Separate the certification process for ease of use and for security
Testing	• The federal government should establish a program for field testing all voting equipment and standard ballot formats.
Management	• Train election officials in the interior workings of their voting equipment.

Source: GAO summary and categorization of Caltech/MIT report.

Caltech/MIT Voting Technology Project: Immediate Steps to Avoid Lost Votes in the 2004 Presidential Election. In July 2004, the Caltech/MIT Voting Technology Project issued a report containing immediate recommendations intended to help the EAC improve the election process for 2004, along with additional recommendations that could have proven more difficult to implement in time for the November 2004 election.[6] While the recommendations were directed at the EAC, many of them were specific enough to be used by state and local election officials; the EAC referenced the report in its tool kit. The report included security and reliability recommendations in the life cycle areas of operations, testing,

[6]Caltech/MIT Voting Technology Project, *Immediate Steps to Avoid Lost Votes in the 2004 Presidential Election: Recommendations for the Election Assistance Commission* (Pasadena, Calif., July 2004). http://www.vote.caltech.edu/media/documents/EAC.pdf (downloaded Oct. 1, 2004).

and management. Some example recommendations from the report are listed in table 12.

Table 12: Caltech/MIT Security and Reliability Practices for Electronic Voting Systems

Life cycle activity	Example practice
Operations	• The EAC should require from each election jurisdiction (county and state) a report of total ballots cast and votes cast for each federal office. • All election jurisdictions should also report on the voting technologies they use for precinct and absentee voting in each federal election. • Audit logs of individuals with access to the computer must be performed and retained after each election. • Computers used for elections should be restricted to the sole purpose of election administration, and not used for other purposes. • Every stage of the election process should require that multiple representatives approved by each major party be involved. The areas that need such oversight include purchasing; equipment setup and testing; ballot development; moving, storing, activating, using, shutting down, and accumulating votes from voting equipment; setting up polling places; testing and using registration and back-end software; and designing and deploying education materials for poll workers and election officials. • Election machines (and ballots where ballots exist) should be well secured. Ideally, numbered seals should be used as closures for the equipment. • In-precinct counting machines should not turn off the ballot overvote and error checking features of these machines.
Testing	• Every ballot design should be tested on real voters from the locality where the ballot will be used. This testing must show the ballot to be fully accessible and to allow voters to record their intentions accurately. • All voting machines should be tested and shown to work as designed before use in any election. Machines should show zero counts; show that all controls, indicators and displays work; show that they can accurately record the votes made; and show that any back-up system in them works. After any physical change or software rebuild, the voting machine should be retested and recertified for use. • A random sample of voting machines should be tested in voting mode as though it were the day of the election.
Management	• Poll workers should be trained with procedure-oriented teaching materials and have ways of looking up answers to important questions in a reasonable time. • Election machines should be controlled by the election officials, not the vendors. To do this, officials need to identify, train, and certify representatives who are competent at overseeing voting machines. • All software (including source code) for voting equipment should be placed in escrow in case of questionable election outcomes and made available for independent review.

Source: GAO summary and categorization of Caltech/MIT report.

League of Women Voters: Safeguarding the Vote. In July 2004 the League of Women Voters produced a report[7] containing recommendations to local election officials that were intended to advance security through, for example, enhanced transparency of the elections and improved voting system testing and physical security. In addition, this report provided advice specific to different types of voting systems. The recommendations related to the security and reliability of electronic voting systems fall in the life cycle activities of operations, testing, and management. Example recommendations from the report are listed in tables below. Table 13 provides examples relevant to all voting systems, table 14 provides examples relevant to optical scan systems, and table 15 provides examples relevant to DRE systems.

Table 13: League of Women Voters Security and Reliability Practices for All Voting Systems

Life cycle activity	Example practice
Operations	• Require bipartisan or third-party monitoring of sensitive election procedures. • Require tracking and documentation of all procedures from the testing of machines to the handling of ballots. • Restrict physical access to all components of voting systems. • Ballots, voting machines, memory cartridges, and counting machines should never be left unattended. • Preferably two election officials will oversee all processes, including the transfer of ballots and other election materials to the central office. • Design a routine process that checks for problems that may have occurred but not been visible on election day; an audit of the election after election day will provide the public with additional assurance that all votes were counted properly and accurately, as well as alert election officials to problems that occurred that may not have surfaced on election day. • Maintain and operate voting systems in isolation from networks and the Internet.
Testing	• Require that all systems, at a minimum, have been state certified and meet all federal voluntary voting system standards. • Test every voting machine to ensure it is operating properly. • Perform uniform, public testing of voting systems. • Test voting machines and counting machines, including their hardware and software, before election day. Carry out testing in a public process.

[7]Tracy Warren, Kelly Ceballos, Lloyd Leonard, and Jeanette Senecal, *Helping America Vote: Safeguarding the Vote* (Washington, D.C.: League of Women Voters, July 2004). http://www.lwv.org/elibrary/pub/voting_safeguarding_color.pdf (downloaded Dec. 13, 2004).

(Continued From Previous Page)

Life cycle activity	Example practice
Management	• Educate voters on the use of all voting equipment both in advance of the election and in the polling place on election day. • Establish statewide practices for the management and operation of voting systems. • Provide adequate training for all election day workers, including ensuring the physical security of the voting system and other voting system security vulnerabilities and countermeasures. • Do not remove machines from the polls for repairs or for any other reason until voting has ended. • Provide a back-up plan in the event of machine failure. • Establish statewide practices for the management and operation of voting systems. • Verify that the electronic and optical scan machines used are the same as the systems that were certified.

Source: GAO summary and categorization of League of Women Voters report.

Table 14: League of Women Voters Security and Reliability Practices for Optical Scan Voting Systems

Life cycle activity	Example practices
Testing	• Ensure that scanners are properly calibrated before election day.
Management	• Both in-person and absentee voters should receive instructions on what constitutes a spoiled ballot and what to do if they spoil their ballot. • Establish procedures for determining voter intent using uniform vote counting standards and for counting ballots that cannot be scanned. The process for counting ballots should be open and conducted under bipartisan scrutiny.

Source: GAO summary and categorization of League of Women Voters report.

Table 15: League of Women Voters Security and Reliability Practices for Direct Recording Electronic Voting Systems

Life cycle activity	Example practices
Operations	• On election day, periodically check to make sure machines are properly calibrated and that cords remain plugged into their sockets. • Configure the polling place to allow full view by poll workers of voting and voter activity to guard against unauthorized access while protecting voter privacy.
Testing	• Test audio and magnification systems for each machine.

Source: GAO summary and categorization of League of Women Voters report.

Numerous Reports Recommended Mitigation Steps. In addition to highlighting problems and concerns, several of the reports we reviewed identified specific measures designed to mitigate or otherwise address the weaknesses in the security and reliability of electronic voting systems. Some reports called on states and local governments to implement both administrative and procedural safeguards to address security and reliability on a comprehensive basis, as well as policies to address specific

weaknesses. In other cases, reports indicated that vendors needed to redesign their systems in order to fix identified technical deficiencies or physical security weaknesses in their products. Table 16 lists mitigation measures identified in the reports we reviewed.

Table 16: A Compendium of Recommended Mitigation Measures to Address Selected Concerns with Electronic Voting Systems' Security and Reliability

Identified concern	Proposed mitigation measure
Jurisdictions may lack an information security management program for electronic voting systems.	Develop and execute a security management plan that includes provisions for • conducting appropriate security training; • ensuring that employees and contractors had proper certifications; • defining security roles and responsibilities; • performing audits according to a well-defined process; • managing passwords effectively, especially on systems with hard-coded passwords or weak password controls; • controlling physical access to systems with weaknesses in their system access controls; and • controlling the use of personal computer memory cards and smart cards for systems that did not protect such devices.
Controls for protecting cast ballots, audit logs, ballot definition files, and other vital data elements are weak.	• Redesign the voting system to provide encryption for these components. • Develop administrative procedures to tightly govern access to the voting terminals, smart cards, and computers used to store accumulated votes and other vital data.
System has network or modem connections that are subject to external network attacks.	• When using network or modem connections, (1) encrypt transmissions, (2) update with anti-virus protection, and (3) develop administrative procedures to minimize the use of such connections.
Power or poll-closing switches are exposed and vulnerable to accidental or intentional triggering.	• Apply a lockable protective seal to cover such buttons. • Redesign the voting system to make such functionality password protected.
The voting system may contain malicious code that could corrupt votes.	• Redesign the system to include a voter-verified paper audit trail for each vote cast.

Source: GAO analysis of recent reports and studies.

Summary of Selected Guidance on Information Technology Security and Reliability

The federal government and other entities have published broad guidance intended to help organizations develop, evaluate, and manage information technology systems in a secure and reliable manner. We have identified examples of such guidance issued by ourselves and six other organizations: National Institute of Studies and Technology (NIST), the Information Systems Security Engineering Association, the Computer Emergency Response Team (CERT) Coordination Center at the Software Engineering Institute (SEI), the SysAdmin, Audit, Network, Security (SANS) Institute, the Institute for Electrical and Electronics Engineers (IEEE), and the American Institute of Aeronautics and Astronautics (AIAA). These are summarized below. As technology continues to evolve and these guidance documents are updated to address emerging issues, stakeholders in voting systems must ensure that their own standards and practices are upgraded to keep pace.

Federal Information System Controls Audit Manual (FISCAM).[1] In January 1999, we issued guidance for reviewing information system controls that affect the integrity, confidentiality, and availability of computerized data. Designed for use by information system auditors, FISCAM defines six major categories of general controls: entitywide security program planning and management; access controls; application software development and change controls; system software; segregation of duties; and service continuity. For each category, FISCAM identifies critical elements essential for establishing adequate controls. State and local jurisdictions acquiring new voting systems or evaluating controls associated with existing systems may use the guidance from FISCAM to make purchasing decisions or to set administrative policy or procedures.

GAO: Information Security Risk Assessment: Practices of Leading Organizations. Our Information Security Risk Assessment guide[2] is intended to help federal managers implement an ongoing information security risk assessment process by providing case studies containing examples of practical risk assessment procedures that have been successfully adopted by organizations. It also identifies critical success factors important to the success of a risk assessment program, such as the involvement of senior management, defined procedures for conducting the

[1]GAO, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999).

[2]GAO, *Information Security Risk Assessment: Practices of Leading Organizations*, GAO/AIMD-00-33 (Washington, D.C.: November 1999).

assessments, and documenting and maintaining the risk assessment results.

NIST: Computer Security Special Publications. The NIST Computer Security Division has published several guides promoting information security development and management practices. These guides address topics such as information security management, acquisition practices, design and development principles, and operation of information systems. Such guides could be used by vendors and developers for the design and development of secure and reliable voting systems, as well as by states and localities for acquisition practices and information management principles. Examples of NIST publications that address system security and reliability are listed in table 17.

Table 17: Examples of NIST Publications Addressing System Security and Reliability

NIST Publication	Description
SP 800-12: *An Introduction to Computer Security: The NIST Handbook* (October 1995)	Explains important concepts, cost considerations, and interrelationships of security controls. It is intended to help readers understand their computer security needs and develop a sound approach to the selection of appropriate management, operational, and technical controls.
SP 800-14: *Generally Accepted Principles and Practices for Securing Information Technology Systems* (September 1996)	Describes 8 principles and 14 related practices related to information security. It is designed to serve as a foundation that management, internal auditors, users, system developers, and security practitioners can use to gain an understanding of the basic security requirements most information technology systems should contain and to establish and review information technology security programs.
SP 800-18: *Guide for Developing Security Plans for Information Technology Systems* (December 1998)	Describes a guideline for federal agencies to follow when developing the security plans that document the managerial, technical, and operational controls for information systems. It provides guidance on the general information that all security plans should contain as well as the management, operational, and technical controls that should be considered for both major applications and general support systems.
SP 800-23: *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products* (August 2000)	Provides guidelines for federal organizations' acquisition and use of security-related information technology products. It recommends that agencies become aware of the benefits of testing products against customer, government, or vendor-developed specifications; consider the risk environment, cost-effectiveness, assurance level, and security functional specifications when selecting information technology products; procure and deploy products that have been independently evaluated and tested against appropriate security specifications, and configure and integrate technology products to ensure that security is appropriately addressed throughout the system.
Federal Information Technology Security Assessment Framework (November 2000)	Identifies five levels of information technology security program effectiveness that measure specific management, operational, and technical control objectives. It is intended to help agency officials determine the current status of their security programs relative to existing policy and to establish a target for improvement. It may be used to assess the status of security controls for information systems.

(Continued From Previous Page)

NIST Publication	Description
SP 800-26: *Security Self-Assessment Guide for Information Technology Systems* (November 2001)	Provides guidance on applying the Federal Information Technology Security Assessment Framework through a questionnaire containing specific control objectives and suggested techniques against which the security of information systems can be measured.
SP 800-27, Rev. A: *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)* (June 2004)	Presents a list of 33 system-level security principles to be considered in the design, development, and operation of information systems. These principles are derived from the concepts defined in SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, and are intended to be used throughout the system life cycle or to help organizations affirm the security posture of already deployed systems. They primarily focus on technical controls, but they also consider nontechnical issues in system security design such as policy, operational procedures, and training.
SP 800-30: *Risk Management Guide for Information Technology Systems* (July 2002)	Provides guidance to information technology personnel on the development of an effective risk management program by providing the definitions and the practical guidance necessary for assessing and mitigating risks identified within information technology systems, and by providing information on the selection of cost-effective security controls. It describes a methodology, a process, and a practice needed for conducting risk assessment, risk mitigation, and risk evaluation and assessment.
SP 800-34: *Contingency Planning Guide for Information Technology Systems* (June 2002)	Provides instructions, recommendations, and considerations for government organizations to consider when developing a plan for recovery of information technology services following an emergency or system disruption. It contains specific contingency planning recommendations for multiple information system platforms and provides strategies and techniques common to all systems.
SP 800-37: *Guide for the Security Certification and Accreditation of Federal Information Systems* (May 2004)	Provides guidelines for the security certification and accreditation of information systems supporting the federal government. It presents a four-phase process for security certification and accreditation, with each phase containing specific tasks and subtasks, which is intended to enable consistent assessments of system security controls, promote understanding of risks resulting from the operation of information systems, and facilitate more informed security accreditation decisions by providing more complete information to authorizing officials.
SP 800-50: *Building an Information Technology Security Awareness and Training Program* (October 2003)	Provides guidelines for building and maintaining a comprehensive awareness and training program, as part of an organization's information technology security program. The guidance is presented in a life cycle approach, ranging from designing, developing, and implementing an awareness and training program, through postimplementation evaluation of the program. It includes guidance on how information technology security professionals can identify awareness and training needs, develop a training plan, and get organizational buy-in for the funding of awareness and training program efforts.
SP 800-53: *Recommended Security Controls for Federal Information Systems* (February 2005)	Provides guidelines for selecting and specifying security controls for federal information systems. It describes a process for selecting and specifying security controls for information systems, catalogs specific security controls organized into management, operational, and technical controls, and summarizes the minimum controls needed for low-impact, moderate-impact, and high-impact systems.
SP 800-55: *Security Metrics Guide for Information Technology Systems* (July 2003)	Provides guidance for the specific development, selection, and implementation of system-level metrics to be used to measure the performance of information system security controls and techniques. It describes the process for development of useful metrics and how to implement a metrics program, as well as presenting a list of example security metrics that can be used or modified to meet specific organizational requirements.

(Continued From Previous Page)

NIST Publication	Description
SP 800-61: *Computer Security Incident Handling Guide* (January 2004)	Assists organizations in establishing a computer security incident response capability and handling incidents efficiently and effectively. It also presents requirements and recommendations that organizations should implement in order to facilitate effective incident response and provides guidance in handling specific types of incidents.
SP 800-64, Revision 1: *Security Considerations in the Information System Development Life Cycle* (June 2004)	Presents a framework for incorporating security across the life cycle of a system and describes a minimum set of security steps needed to effectively incorporate security into a system during its development. It is intended to help agencies select and acquire cost-effective security controls by explaining how to include information system security requirements in the system development life cycle.
SP 800-70: *Security Configuration Checklist Program for IT Products—Guidance for Checklist Users and Developers* (May 2005)	Describes a program for facilitating the development and sharing of security configuration checklists so that organizations and individual users can better secure their information technology products. It is intended to provide a framework for developers to submit checklists to NIST; to assist developers by providing a consistent approach to securing different types of systems that are connected to the same environments; to assist developers and users by providing guidelines for making checklists better documented and more usable; to provide a managed process for the review, update, and maintenance of checklists; and to provide an easy-to-use national repository of checklists.

Source: NIST.

CERT/CC: Security Improvement Modules. The CERT Coordination Center (CERT/CC) at the Software Engineering Institute at Carnegie Mellon University provides a series of Security Improvement Modules and associated practices[3] intended to help system and network administrators improve the security of their information systems and networks. The modules contain practices and recommendations in such areas as the outsourcing of security services, implementing system security, detecting and responding to intrusions, and securing system hardware.

International Systems Security Engineering Association: Systems Security Engineering Capability Maturity Model (ISO/IEC 21827). The International Systems Security Engineering Association promotes and maintains the Systems Security Engineering Capability Maturity Model (SSE-CMM)®. Version 3.0 of the SSE-CMM was issued in June 2003. The SSE-CMM is a process reference model describing the requirements for implementing security in information systems. It describes security engineering activities for secure product definition, design, development, and operation and requirements for developers, system integrators, information security providers, and engineers. It identifies a comprehensive framework with associated security engineering activities

[3]CERT Coordination Center, *CERT® Security Improvement Modules* (Carnegie Mellon University, undated), http://www.cert.org/security-improvement/.

designed to help provide a method by which system developers can measure and improve performance in the application of security engineering principles.

SANS Institute: Resources and Guidance. The SANS Institute, established in 1989 as a cooperative research and education organization, provides a variety of resources to help organizations implement and improve system security. Its Web site[4] provides guidance on writing information security policies and offers templates for organizations to use in developing their own policies. SANS also offers the Information Security Reading Room,[5] a collection of research documents on various aspects of information security. The documents address a variety of information security topics, such as security basics, information assurance, wireless access, physical security, and disaster recovery. They could be used by states and local election administrators as a resource to set security policies or create procedures for handling security and reliability problems. SANS also offers a security awareness training program and publishes a list of common security vulnerabilities.

IEEE Std 1332-1998: IEEE Standard Reliability Program for the Development and Production of Electronic Systems and Equipment. This standard is intended to encourage suppliers and customers to cooperatively integrate their reliability processes and to establish a contractual or obligatory relationship that promotes reliability management. It is intended to help guide suppliers in developing a reliability program that meets the needs of the customer through meeting three objectives: determining the customer's requirements, determining a process to satisfy those requirements, and verifying that the customer's requirements and product needs are met. Further, it describes activities that both the customer and the supplier should perform to meet these objectives.

ANSI/AIAA R-013-1992: Recommended Practice for Software Reliability. This recommended practice defines a methodology for software reliability engineering. It describes activities and qualities of a software reliability estimation and prediction program, presents a framework for risk assessment and failure rate prediction, recommends models for estimation

[4]SANS, www.sans.org.

[5]SANS, www.sans.org/rr/.

and prediction of software reliability, and specifies mandatory as well as recommended software reliability data collection requirements. It is intended to support the design, development, and testing of software, including activities related to software quality and software reliability, as well as to serve as a reference for research on the subject of software reliability.

Resolutions Related to Voting System Security and Reliability

The Election Assistance Commission's (EAC) Technical Guidelines Development Committee (TGDC) has approved 41 resolutions to improve current voluntary voting system standards. Of the 41 resolutions, 24 have potential to improve the security and reliability of electronic voting systems. Table 18 provides information on these 24 resolutions including our determination of their relevance to security and reliability goals, TGDC's priorities for resolutions related to the development of voluntary voting system guidelines (VVSG), and the version of guidelines that is expected to address each resolution. The table shows that the majority of the 24 resolutions—including three high-priority resolutions—are not expected to be fully addressed in the 2005 update to the voting standards. Instead, most are expected to be addressed in a future version.

Table 18: Resolutions Related to Security and Reliability of Electronic Voting Systems and Plans for Implementing Them in Future Standards

Resolution number	Date approved	Resolution title	Goal: Improve security	Goal: Improve reliability	TGDC priority	2005 VVSG	Future VVSG
05-04	07/09/04	Certified Software for the National Software Reference Library	○	○	not prioritized	#	#
03-05	01/19/05	Human Factors and Privacy of Voting Systems at the Polling Place	–	○	1,2	▼	◆
08-05	01/19/05	Usability Guidance for Instructions, Ballot Design, and Error Messages	–	○	2	#	◆
09-05	01/19/05	General Voting System Human Factors and Privacy Considerations	○	○	1,2	▼	◆
12-05	01/19/05	Voter Verifiability I	●	–	1,2	▼ V	◆
14-05	01/19/05	Commercial Off-the-Shelf Software	●	–	2	#	◆
15-05	01/19/05	Software Distribution	●	○	1	▼	◆
16-05	01/19/05	Setup Validation	○	○	1	▼	◆
17-05	01/19/05	Testing (for Security)	●	○	2	#	◆
18-05	01/19/05	Documentation (for Security)	●	○	2	#	◆
21-05	01/19/05	Multiple Representations of Ballots	○	●	2	▼ V	◆
22-05	01/19/05	Federal Standards	●	-–	2	▼	◆
23-05	01/19/05	Common Ballot Format Specifications	●	–	3	▼ V	◆
24-05	01/19/05	Conformance Clause	○	○	1,2	▼	◆
25-05	01/19/05	Precise and Testable Requirements	○	●	2	#	◆

(Continued From Previous Page)

Resolution number	Date approved	Resolution title	Goal: Improve security	Goal: Improve reliability	TGDC priority	2005 VVSG	Future VVSG
26-05	01/19/05	Uniform Testing Methods and Procedures	○	○	2	#	◆
27-05	01/19/05	Non-Conformant Voting Systems	○	○	2	#	◆
29-05	01/19/05	Ensuring Correctness of Software Code	○	○	2	#	◆
30-05	01/19/05	Quality Management Standards	●	○	3	#	◆
32-05	01/19/05	Sharing Information and De-Qualification of Voting Systems	●	●	3	#	#
33-05	01/19/05	Glossary and Voting Model	○	○	1,2	▼	◆
35-05	01/19/05	Wireless	●	–	1	▼	◆
36-05	03/09/05	Consensus Standards	○	○	not prioritized	#	◆
39-05	04/21/05	Voter-Verified Paper Audit Trail Assignment	○	○	not prioritized	#	#

Source: GAO analysis of NIST and TGDC data.

Key:

Columns 4 and 5

● Resolution specifically identifies the goal
○ Resolution facilitates achievement of the goal
– Resolution is not essential to the goal

Columns 7 and 8

◆ Expected to be fully addressed in publication
▼ Expected to be partially addressed in publication
V Supports voter-verified paper audit trail implementation
Not expected to be addressed in publication

Comments from the Election Assistance Commission

U.S. ELECTION ASSISTANCE COMMISSION
1225 New York Ave. NW – Suite 1100
Washington, DC 20005

September 13, 2005

Mr. David A. Powner, Director
Information Technology Management Issues
Mr. Randolph C. Hite, Director
Information Technology Architecture and Systems
United States Government Accountability Office

RE: Draft Report GAO 05-956, *Elections: Federal Efforts To Improve Security and Reliability of Electronic Voting Systems are Under Way, but Key Activities Need to be Completed*

Thank you for the opportunity to comment on draft GAO Report 05-956. The EAC appreciates the time and effort put forth by GAO during the preparation of this document and the willingness of GAO staff to discuss pertinent issues at length with the EAC, NIST and other key players in the election community. As you know this letter follows a combined exit conference and discussion of GAO's draft report. Because our meeting was scheduled late in the process, there may be some comments set forth below that have already been addressed.

It is apparent from our review of the draft report that GAO has taken steps in this engagement to understand the election process in addition to evaluating the electronic voting systems in use in that process. EAC is also pleased that GAO recognizes and highlights the decentralized nature of the election process in the United States, the intricacies this decentralization brings to our election system and the critical roles played by local, state and Federal election officials in this process.

While the overall quality of the report is quite high, the EAC does have some issues we feel need to be addressed prior to the final publication of this document. During our September 7, 2005 meeting, we highlighted and provided to you a list of technical corrections to the facts as stated in the draft report. For your convenience, a copy of that list, as amended based upon the conversations in that meeting, has been attached to this letter. (Appendix "1")

GENERAL COMMENTS

GAO's draft report does not refer to sources.

Although the bibliography in Appendix V of the report lists numerous studies on the security and reliability of electronic voting, few if any, of these studies are cited or footnoted within the body of the report. The report generally refers to "security experts and others" without providing any specific reference to the individual sources or the reports on which the statements that follow such generalities are based. Including specific citations where appropriate would lend much needed support to various broad statements and generalizations made throughout the report regarding the lack of security and reliability of electronic voting systems.

GAO's draft report does not give context to the identified security and reliability issues.

GAO identifies several incidences of voting system security or reliability problems. However, the report does not provide a context of the pervasiveness or relative obscurity of these issues. There is no statistical evidence offered as to how frequently these issues arise or whether problems occur in a large or small percentage of electronic voting system usage. While it has been offered by GAO that these reported problems or issues systemic, the report fails to identify whether the identified problems are voting system specific, jurisdiction specific, or cross lines of both manufacturers and voting jurisdictions.

GAO's draft report reflects significant reliance on reports produced by others without substantiation of the claims made in those reports.

The EAC is concerned about instances of electronic voting system failures highlighted in the report that do not appear to have been thoroughly researched and analyzed. As an example page 26 or the report states, in part, that:
"…computer security experts working with a local election supervisor in Florida demonstrated that someone with access to an optical scan voting system could falsify election results without leaving any record of this action in the system's audit logs by using altered memory cards." This statement should be verified with election officials and voting systems experts at the state level in Florida to assure its accuracy, and to get a full understanding of the details and validity of this so-called "demonstration."

In another example, on page 25 of the draft report, GAO relies on the reports contained in its bibliography to state that there are no significant concerns with security or reliability at the acquisition phase of the voting system life cycle. Conversations with state and local election officials that have recently purchased electronic voting equipment would reveal that a significant number of voting systems are rejected during the acceptance testing phase of acquisition. While this may not point to a security concern, it does demonstrate a quality assurance or reliability concern.

2

EAC is but one participant in the process of assuring reliability and security of voting systems.

While GAO has done a good job with recognizing that the decentralization of elections in this country -- that is federal elections as well as state elections are administered by state and local election officials – the report fails to capture EAC's role in the improvement to security and reliability of electronic voting systems. EAC is the federal agency responsible for establishing a uniform set of guidelines (testing standards) against which voting systems can be measured. EAC, its advisory committee – the Technical Guidelines Development Committee --, and the National Institute of Standards and Technology are working diligently to develop a revised set of voting system guidelines. However, the guidelines are only one piece of the puzzle. It is the voting system vendors that must design and configure their systems to meet those guidelines and the state and local election officials that must adopt these guidelines and restrict their purchases of voting systems to those that conform to the guidelines. GAO's draft report focuses exclusively on EAC as the answer to the questions surrounding electronic voting. In reality, EAC simply cannot change the security and reliability of voting systems alone.

TECHNICAL COMMENTS

At our meeting on September 7, 2005, EAC identified a number of technical corrections related to specific facts or statements made in the report. In addition to the items enumerated in writing, our discussions produced several other technical errors that needed correction. For your convenience, an updated list of technical comments has been attached to this letter as Appendix "1".

RESPONSES TO GAO RECOMMNEDATIONS

The EAC agrees with GAO that the implementation of the five recommendations presented in this report will improve the voting process and the public perception regarding the security and reliability of electronic voting systems. Prior to the issuance of this report and prior to EAC receiving a draft of this report, EAC took significant steps toward accomplishing the very processes, procedures and methods recommended by GAO. Provided below is additional information concerning EAC's efforts relative to each of the five recommendations.

Recommendation 1: Collaborate with NIST and the Technical Guidelines Development Committee to define specific tasks, measurable outcomes, milestones, and resource needs required to improve the voting system standards that affect security and reliability of voting systems.

NIST and EAC have begun to define specific tasks and outcomes for subsequent iterations of the VVSG document. These issues will be discussed in detail during the TGDC Plenary Session on September 29, 2005 in Boulder, Colorado. A crucial task which will allow both EAC and NIST to most effectively direct

scarce resources and to prioritize upcoming tasks is the development of a comprehensive vulnerability analysis of electronic voting systems. NIST and the U.S. election community will begin gathering threat analysis material and information during the upcoming meeting on this topic scheduled for October 7, 2005 at the NIST complex in Gaithersburg, Maryland.

Recommendation 2: Expeditiously establish documented policies, criteria, and procedures for certifying voting systems that will be in effect until the national laboratory accreditation program for voting systems becomes fully operational; define tasks and time frames for achieving the full operational capability of the national voting system certification program.

EAC began the initial transition of the voting system testing and certification program as required by HAVA by adopting at its August 23, 2005 public meeting a frame work for the interim and future voting system certification processes. A copy of the document describing the processes that was adopted by the Commission is attached as Appendix "2".

The initial task in the interim certification process will be a two-part transition of the current NASED accredited ITA's to the EAC. Part one will be a simple documentation and transition process which will allow the current ITA's to continue testing voting systems to the 2002 VSS. Part two of this task will provide for an interim accreditation process to ensure that these labs are competent to test to the new requirements of the 2005 VVSG once that document has been adopted by EAC.

By October 1, 2005, EAC will begin registering those vendors who intend to have systems evaluated through the EAC conformance testing process. An integral component of the EAC's vendor registration process will be a requirement that vendors notify EAC of problems encountered with their certified products in the field and to suggest solutions to any problem encountered. Resources permitting, EAC will consider options to enhance this program to include investigation and analysis of reported voting system problems and methods of communicating these issues to the entire election community.

During this same timeframe, EAC will initiate contractual agreements with a group of technical experts for the review of voting system test reports. By January 1, 2006, EAC will be in a position to fully implement conformance testing of voting systems and to begin the process of issuing voting system certifications.

Recommendation 3: Improve management support to state and local election officials by collaborating with NIST to establish a process for continuously updating the National Software Reference Library for voting system software; take effective action to promote the library to state and local governments; identify and disseminate information on resources to assist state and local governments with

using the library; and assess use of the library by states and local jurisdictions for the purpose of improving library services.

In 2005, EAC contracted with NIST to develop an interface to the National Software Reference Library (NSRL) that would be more readily usable by the state and local election officials. See MOU with NIST attached as Appendix "3". In addition, EAC and NIST seek through the same agreement to expand the capabilities of the NSRL to allow users to verify not only EMS software but also software that has been installed and used on a voting system.

In 2004, EAC began the effort of encouraging voting system vendors to submit their software versions to the NSRL for cataloguing. Upon the transition of voting system certification to EAC, EAC will require all vendors who submit voting systems for certification to file their software with NSRL.

Recommendation 4: Improve management support to state and local election officials by collaborating with TGDC and NIST to develop a process and associated timeframes for sharing information on the problems and vulnerabilities of voting systems.

In its framework for the voting system certification process, EAC has contemplated the need for information relative to the strengths and weaknesses, certification and decertification of voting systems. As such, EAC will introduce additional transparency to the process of voting system certification and decertification. In addition, EAC has demonstrated its desire to gather and disseminate data regarding voting system problems in its 2004 Election Day Survey. Results of that survey will be released this month and will identify voting system problems that occurred on election day, as reported by the 50 states and 5 territories.

Recommendation 5: Improve management support to sate and local election officials by establishing a process and schedule for periodically compiling and disseminating recommended practices related to security and reliability management throughout the system life cycle (including the recommended practices identified in this report) and ensuring that this process uses information on the problems and vulnerabilities of voting systems.

In 2005 and 2006, EAC and the National Association of State Election Directors (NASED) will work together to develop a comprehensive set of management guidelines that will accompany the Voluntary Voting System Guidelines. Testing voting systems for conformance to uniform standards is only half of the equation involved with administering secure elections. The management processes, physical security, and protocols used to accept, program, test and maintain voting systems is an equally important part of conducting fair and accurate elections. The management guidelines to be developed by EAC and NASED will focus on these issues.

5

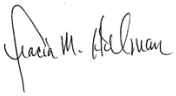
The United States Election Assistance Commission would like to take the opportunity to thank GAO for its work, dedication and concern about the technology and processes that underlie one of America's most precious freedoms, the right to vote. EAC and GAO join the legions of election officials throughout the country that work tirelessly to conduct free, fair and accurate elections.

It has been our pleasure to work with GAO on this historic study and analysis of our country's voting systems. It is critical that the federal government and our state and local counterparts analyze the means by which we conduct elections with the goal of always improving public confidence and security in our election process. We hope that the comments offered today will be of assistance to GAO and lend to the applicability and credibility of its report.

Congress and the nation can rest assured that EAC will continue is vigilant efforts to help our nation's election officials implement the requirements of the Help America Vote Act of 2002 and to work to continually improve our elections.

Sincerely,

Gracia Hillman, Chair



Paul DeGregorio, Vice Chairman

Ray Martinez, III

Donetta Davidson

6

Comments from the National Institute of Standards and Technology

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899-0001
OFFICE OF THE DIRECTOR

SEP 0 9 2005

Ms. Paula Moore
Senior Analyst
United States Government Accountability Office
Washington, D.C. 20548

Dear Ms. Moore:

Thank you for the opportunity to comment on the draft report entitled *Elections: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to be Completed* (GAO-05-956). We agree wholehcartedly with the report's conclusions that specific tasks, processes, and time frames must be established to improve the national voting systems standards, testing capabilities, and management support available to state and local election officials.

The 2002 Help America Vote Act (HAVA) established the Technical Guidelines Development Committee (TGDC) to assist the Election Assistance Commission (EAC) with the development of voluntary voting system guidelines. HAVA directs the Commerce Department's National Institute of Standards and Technology (NIST) director to chair the TGDC and to provide technical support to the TGDC in the development of these guidelines. The enclosed comments provide additional details on DOC/NIST efforts with respect to the security and reliability of electronic voting systems.

Sincerely,

William Jeffrey

William Jeffrey

Enclosure

NIST

GAO Contacts and Staff Acknowledgments

GAO Contacts

David A. Powner, (202) 512-9286 or pownerd@gao.gov
Randolph C. Hite, (202) 512-3439 or hiter@gao.gov

Staff Acknowledgments

In addition to those named above, Mark Braza, Barbara Collier, William Cook, Dan Gordon, Richard Hung, Kevin Jackson, Stanley Kostyla, Linda Lambert, Paula Moore, Colleen Phillips, Jay Smale, Amos Tevelow, and Jessica Waselkow made key contributions to this report.

Bibliography

We selected the following reports, analyses, testimonies, and other documents because of their relevance to the security and reliability of electronic voting systems. We used this literature to identify concerns and recommended practices involving the security and reliability of voting systems. The first list comprises reports and studies that include concerns about the security and reliability of voting systems; the second list comprises reports and studies that include recommended practices for improving the security and reliability of voting systems. There was some overlap between the lists in that some of the reports that identified concerns also suggested mitigating measures to address these concerns. These mitigating measures are summarized in appendix II, table 16.

The two lists of studies and reports are not intended to be an exhaustive compilation of available information or literature in this area, nor does the presence of a document in these lists imply that it is endorsed or otherwise recommended. These lists identify primary sources. Supplementary and corroborating information was gathered from other reports, testimonies, and through interviews with experts.

Reports and Studies that Include Concerns About the Security and/or Reliability of Voting Systems

[1] Coggins, Carolyn, and Gail Audette, SysTest Labs, LLC. "NASED Independent Test Authority Qualification Testing" (Testimony before the Environment, Technology, and Standards Subcommittee of the U.S. House of Representatives' Committee on Science, May 2004). http://www.house.gov/science/hearings/ets04/jun24/coggins.pdf (downloaded July 18, 2005).

[2] Compuware Corporation. *Direct Recording Electronic (DRE) Technical Security Assessment Report* (prepared for the Ohio Secretary of State, November 2003). http://www.sos.state.oh.us/sos/hava/files/compuware.pdf (downloaded October 1, 2004).

[3] Compuware Corporation. *Diebold Direct Recording Electronic (DRE) Technical Security Re-Assessment Report* (prepared for the Ohio Secretary of State, August 2004). http://www.sos.state.oh.us/sos//hava/files/DieboldReassessment.pdf (downloaded July 18, 2005).

[4] Coulter, Michael (Chair), Independent Election Committee. *Restoring Confidence to Voters: Findings and Recommendations of the Independent Election Committee* (Mercer County, Penn., February 2005).

http://elections.ssrc.org/data/mercer_co_commission_findings.pdf (downloaded July 20, 2005).

[5] Department of State (Pennsylvania), *Reexamination Results of Unilect Corporation's PATRIOT Direct Recording System* (April 2005). http://www.dos.state.pa.us/dos/lib/dos/20/dos_report_unilect_system.pdf (downloaded August 8, 2005).

[6] Franklin County Board of Elections. *Election 2004: A Report to the Community* (Franklin, County, Ohio, undated). http://www.electionline.org/Portals/1/Resource%20Library/Franklin.County.OH.2004.pdf (downloaded July 18, 2005)

[7] Hursti, Harri. *The Black Box Report: SECURITY ALERT July 4, 2005, Critical Security Issues with Diebold Optical Scan Design* (Renton, Wash., July 2005). http://www.blackboxvoting.org/BBVreport.pdf (downloaded July 5, 2005)

[8] InfoSENTRY Services, Inc. *Computerized Voting Systems Security Assessment: Summary of Findings and Recommendations*, volume 1 (prepared for the Ohio Secretary of State, November 2003). http://www.sos.state.oh.us/sos/hava/files/InfoSentry1.pdf (downloaded October 1, 2004).

[9] International Foundation for Election Systems. *Unified Monitoring Report to the Center for Democracy (CFD): International Foundation for Election Systems (IFES) Team Members, Miami-Dade County, Florida* (Washington, D.C., November 2002). http://www.reformcoalition.org/Ressources/CFD%20miami%20dade%20final%20report.pdf (downloaded July 18, 2005).

[10] Jones, Douglas W. *Comments on the FEC's Draft Voting System Standards as revised, Dec 13, 2001* (Submitted to the Federal Election Commission, Jan. 2002). http://www.cs.uiowa.edu/~jones/voting/fec1.html (downloaded June 3, 2005).

[11] Jones, Douglas W. *Added Comments on the FEC's Voting System Standards* (Submitted to the Federal Election Commission, Feb. 2002). http://www.cs.uiowa.edu/~jones/voting/fec2.html (downloaded June 3, 2005).

[12] Jones, Douglas W. *Voting Systems Standards Work That Remains To Be Done* (Testimony before the Federal Election Commission, April 2002). http://www.cs.uiowa.edu/~jones/voting/fec3.html (downloaded June 3, 2005).

[13] Kohno, Tadayoshi, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach. *Analysis of an Electronic Voting System* (paper prepared for the IEEE Symposium on Security and Privacy, February 2004). http://avirubin.com/vote.pdf (downloaded July 18, 2005).

[14] Marendt, Candace (Chairman); Steve Eichholtz (Vice-Chairman); Doris Anne Sadler (Secretary): Marion County Board of Elections. *Marion County Election Board Minutes: Emergency Meeting* (Marion County, Ind., April 2004). http://www.indygov.org/NR/rdonlyres/emkiqfxphochfss2s5anfuxbgj3zgpkv557moi3rb6f3ne44mcni2thdvoywyjcigyeoykwru53mopaa6kt2uxh7ofe/20040422.pdf (downloaded July 18, 2005).

[15] Mercuri, Rebecca. *The FEC Proposed Voting Systems Standard Update: A Detailed Comment by Dr. Rebecca Mercuri* (Submitted to the Federal Election Commission, Sept. 2001). http://www.notablesoftware.com/Papers/FECRM.html (downloaded June 2, 2005).

[16] Miami-Dade Election Reform Coalition. *Get It Right The First Time: Poll Closing Observation, Ballot Accounting, and Electronic Voting Security* (Miami, Fla., May 2005). http://www.reformcoalition.org/Ressources/GetItRightTheFirstTime.pdf (downloaded July 20, 2005).

[17] Miami-Dade County Office of Inspector General. *OIG Final Report: Miami-Dade County Voting Systems Contract No. 326* (Miami, Fla., May 2003). http://www.miamidadeig.org/reports/voting%20final%20report.pdf (downloaded December 13, 2004).

[18] Office of the Secretary of State (California). *Secretary of State's Ad Hoc Touch Screen Task Force Report* (July 2003). http://www.ss.ca.gov/elections/taskforce_report_entire.pdf (downloaded October 1, 2004).

[19] Office of the Secretary of State (California). *Report on the March 2, 2004 Statewide Primary Election* (April 2004).

http://www.ss.ca.gov/elections/ks_dre_papers/ march_2_report_final.pdf (downloaded May 10, 2005).

[20] Office of the Secretary of State (California). *Staff Report on the Investigation of Diebold Election Systems, Inc.* (April 2004). http://www.ss.ca.gov/elections/ks_dre_papers/ diebold_report_april20_final.pdf (downloaded August 22, 2005).

[21] RABA Technologies LLC. *Trusted Agent Report: Diebold AccuVote-TS Voting System* (report prepared for Department of Legislative Services, Maryland General Assembly, Annapolis, Md., January 2004). http://www.raba.com/press/TA_Report_AccuVote.pdf (downloaded October 1, 2004).

[22] Science Applications International Corporation (SAIC). *Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes* (report prepared for State of Maryland, Department of Budget and Management, Office of Information Technology, Annapolis, Md., September 2003). http://www.dbm.maryland.gov/dbm_publishing/ public_content/dbm_search/technology/toc_voting_system_report/votingsystemreportfinal.pdf (downloaded October 1, 2004).

[23] Selker, Ted, and Jon Goler, Caltech/MIT Voting Technology Project. *Security Vulnerabilities and Problems with VVPT* (Cambridge, Mass., April 2004). http://www.vote.caltech.edu/media/documents/vtp_wp13.pdf (downloaded October 1, 2004).

[24] Shamos, Michael. "Testimony of Michael I. Shamos before the Environment, Technology, and Standards Subcommittee of the U.S. House of Representatives' Committee on Science" (Washington, D.C., June 2004). http://www.house.gov/science/hearings/ets04/jun24/shamos.pdf (downloaded July 18, 2005).

[25] Shamos, Michael. *UniLect Corporation PATRIOT Voting System: An Evaluation* (paper prepared for the Secretary of the Commonwealth of Pennsylvania, April 2005). http://www.dos.state.pa.us/dos/lib/dos/20/shamos_report-_unilect200502apr05.pdf (downloaded July 18, 2005).

[26] State Board of Elections (Maryland). *Response to: Department of Legislative Services Trusted Agent Report on Diebold AccuVote-TS Voting System* (Annapolis, Md., January 2004).

http://mlis.state.md.us/Other/voting_system/sbe_response.pdf (downloaded August 20, 2005).

[27] Wallach, Dan S., *Democracy at Risk: The 2004 Election in Ohio. Section VII: Electronic Voting: Accuracy, Accessibility and Fraud.* (Democratic National Committee Voting Rights Institute, June 2005.) http://a9.g.akamai.net/7/9/8082/v001/www.democrats.org/pdfs/ohvrireport/section07.pdf (downloaded July 15, 2005).

Reports and Studies that Recommend Practices for Enhancing Security and Reliability of Voting Systems

Brennan Center for Justice and Leadership Conference on Civil Rights. *Recommendations of the Brennan Center for Justice and the Leadership Conference on Civil Rights for Improving Reliability of Direct Recording Electronic Voting Systems* (Washington, D.C., June 2004). http://www.votingtechnology.org/docs/FinalRecommendations.doc?PHPSESSID=9138d73beb5274b0277759bf57330169 (downloaded August 22, 2005).

Browning, Kurt S., Supervisor of Elections, Pasco County, Florida. *Election Security Procedures*, ver. 1.9 (Dade City, Fla., January 2004). http://www.eac.gov/bp/docs/PascoSecurity.pdf (downloaded July 18, 2005).

Caltech/MIT Voting Technology Project. *Voting—What Is, What Could Be* (July 2001). http://www.vote.caltech.edu/media/documents/july01/July01_VTP_Voting_Report_Entire.pdf (downloaded October 1, 2004).

Caltech/MIT Voting Technology Project. *Immediate Steps to Avoid Lost Votes in the 2004 Presidential Election: Recommendations for the Election Assistance Commission* (Pasadena, Calif., July 2004). http://www.vote.caltech.edu/media/documents/EAC.pdf (downloaded October 1, 2004).

Caltech/MIT Voting Technology Project. *Insuring the Integrity of the Electoral Process: Recommendations for Consistent and Complete Reporting of Election Data* (Pasadena, Calif., October 2004). http://www.vote.caltech.edu/media/documents/auditing_elections_final.pdf (downloaded July 18, 2005).

Election Center. *Accessibility Preparations Checklist* (Houston, Tex., May 2004). http://www.electioncenter.org/ElectionPrep/Accessibility.pdf (downloaded August 18, 2005).

Election Center. *Checklist for Ballot Security* (Houston, Tex., May 2004). http://www.electioncenter.org/ElectionPrep/BallotSecurity.pdf (downloaded August 18, 2005).

Election Center. *Checklist for Polling Place Preparations* (Houston, Tex., May 2004). http://www.electioncenter.org/ElectionPrep/PollingPlacePrep.pdf (downloaded August 18, 2005).

Election Center. *Recount Procedures* (Houston, Tex., May 2004). http://www.electioncenter.org/ElectionPrep/Recount.pdf (downloaded August 18, 2005).

Election Center. *Voting Systems Checklist* (Houston, Tex., May 2004). http://www.electioncenter.org/ElectionPrep/VotingSystems.pdf (downloaded August 18, 2005).

Federal Election Commission. *Usability Testing of Voting Systems* (Washington, D.C., October 2003). http://www.eac.gov/bp/docs/Usability%20Testing%20of%20Voting%20Systems.pdf (downloaded July 18, 2005).

Federal Election Commission. *Developing a User-Centered Voting System* (Washington, D.C., October 2003). http://www.eac.gov/bp/docs/Developing%20a%20User_Centered%20Voting%20System.pdf (downloaded July 18, 2005).

Federal Election Commission. *Procuring a User-Centered Voting System* (Washington, D.C., October 2003). http://www.eac.gov/bp/docs/Procuring%20a%20User_Centered%20Voting%20System.pdf (downloaded July 18, 2005).

Fischer, Eric A., Congressional Research Service. *Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues* (November 2003). http://www.congress.gov/erp/rl/pdf/RL32139.pdf (downloaded October 18, 2004).

Jones, Douglas W. *Recommendations for the Conduct of Elections in Miami-Dade County using the ES&S iVotronic System* (May 30, 2004, revised June 7, 2004). http://www.cs.uiowa.edu/~jones/voting/miami.pdf (downloaded July 18, 2005).

Kennedy School of Government, Harvard University. *Voting, Vote Capture and Vote Counting Symposium: Electronic Voting Best Practices* (summary of the Symposium on Voting, Vote Capture and Vote Counting, June 2004). http://designforvalues.org/voting/votingABP_final.pdf (downloaded December 13, 2004).

National Task Force on Election Reform. *Election 2004: Review and Recommendations by the Nation's Elections Administrators* (Houston, Tex., Election Center, May 2005). http://www.electioncenter.org/frontdocs/Task%20Force%20Report%20Book%202005.pdf (downloaded August 18, 2005).

Saltman, Roy G., National Bureau of Standards. *NBS Special Publication 500-158: Accuracy, Integrity, and Security in Computerized Vote-Tallying* (Gaithersburg, Md., August 1988).

Schmidt, Connie, Election Commissioner, Johnson County Kansas Election Office. *Implementing a Voting System From a Local Election Administrator's Viewpoint* (Olathe, Kans., 2003). http://www.eac.gov/bp/docs/Implementation%20Guidebook.pdf (downloaded July 18, 2005).

Shelley, Kevin, California Secretary of State. *Security Measures for Touch Screen (DRE) Voting Systems for the March Election* (document sent to all County Clerks/Registrars of Voters, Sacramento, Calif., February 2004). http://www.ss.ca.gov/elections/ks_dre_papers/security_measures_implemented_mar04.pdf (downloaded August 22, 2005).

United States Election Assistance Commission. *Best Practices Tool Kit* (July 2004). http://www.eac.gov/bp/docs/BestPracticesToolKit.doc (downloaded October 1, 2004).

Voter Protection Project, Verifiedvoting.org, Electronic Frontier Foundation. *Electronic Voting Machine Information Sheet and Glossary*, ver. 0.4 (August 2004). http://www.eff.org/Activism/E-voting/20040818_InfoSheetGlossary_v0.4.pdf (downloaded July 18, 2005).

Warren, Tracy, Kelly Ceballos, Lloyd Leonard, and Jeanette Senecal, League of Women Voters. *Helping America Vote: Safeguarding the Vote* (Washington, D.C., July 2004). http://www.lwv.org/elibrary/pub/voting_safeguarding_color.pdf (downloaded December 13, 2004).

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER