

September 2005

ELECTIONS

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



G A O

Accountability * Integrity * Reliability

ELECTIONS

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



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 Pownall at (202) 512-9286 or pownald@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

- | | |
|---|---|
| <ul style="list-style-type: none"> • 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. | <ul style="list-style-type: none"> • 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

Letter	1
Results in Brief	2
Background	5
Significant Concerns Have Been Raised about the Security and Reliability of Electronic Voting Systems	22
Recommended Practices Address Electronic Voting Systems' Security and Reliability	38
National Initiatives Are Under Way to Improve Voting System Security and Reliability, but Key Activities Need to Be Completed	43
Conclusions	53
Recommendations for Executive Action	53
Agency Comments and Our Evaluation	54

Appendixes

Appendix I: Objectives, Scope, and Methodology	60
Appendix II: Selected Recommended Practices for Voting System Security and Reliability	63
Appendix III: Summary of Selected Guidance on Information Technology Security and Reliability	78
Appendix IV: Resolutions Related to Voting System Security and Reliability	84
Appendix V: Comments from the Election Assistance Commission	86
Appendix VI: Comments from the National Institute of Standards and Technology	92
Appendix VII: GAO Contacts and Staff Acknowledgments	93

Bibliography	94
--------------	----

Tables	
Table 1: Common Types of Security and Reliability Concerns Viewed in Terms of the Voting System Life Cycle	24
Table 2: Federal Initiatives Related to Improving the Security and Reliability of Voting Systems	44

Table 3: Nongovernmental Initiatives to Improve Voting System Security and Reliability	51
Table 4: EAC Security and Reliability Practices for All Types of Voting Systems	64
Table 5: EAC Security and Reliability Practices for Optical Scan Voting Systems	65
Table 6: EAC Security and Reliability Practices for Direct Recording Electronic Voting Systems	66
Table 7: NIST Security and Reliability Practices for Electronic Voting Systems	67
Table 8: Brennan Center Example Security and Reliability Practices for Direct Recording Electronic Voting Systems	68
Table 9: Election Center Security and Reliability Practices for Elections	69
Table 10: National Task Force on Election Reform Security and Reliability Practices for Voting Systems	71
Table 11: Caltech/MIT Security and Reliability Practices for Voting Systems	73
Table 12: Caltech/MIT Security and Reliability Practices for Electronic Voting Systems	74
Table 13: League of Women Voters Security and Reliability Practices for All Voting Systems	75
Table 14: League of Women Voters Security and Reliability Practices for Optical Scan Voting Systems	76
Table 15: League of Women Voters Security and Reliability Practices for Direct Recording Electronic Voting Systems	76
Table 16: A Compendium of Recommended Mitigation Measures to Address Selected Concerns with Electronic Voting Systems' Security and Reliability	77
Table 17: Examples of NIST Publications Addressing System Security and Reliability	79
Table 18: Resolutions Related to Security and Reliability of Electronic Voting Systems and Plans for Implementing Them in Future Standards	84

Figures

Figure 1: Stages of an Election Process	7
Figure 2: Precinct-Count Optical Scan Tabulator and Central-Count Optical Scan Tabulator	9
Figure 3: Two Types of DRE Systems—Pushbutton and Touchscreen	11

Contents

Figure 4: States Requiring the Use of Federal Voting System Standards and States Requiring National Certification Testing	18
Figure 5: A Voting System Life Cycle Model	20

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.



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

¹GAO, *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.

²GAO'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.

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

⁴California 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).

⁵For 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 standards⁶ 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

⁶The 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.

⁷GAO-02-3