United States Government Accountability Office

GAO

Report to the Chairman, Committee on House Administration, House of Representatives

September 2008

ELECTIONS

Federal Program for Certifying Voting Systems Needs to Be Further Defined, Fully Implemented, and Expanded

GAO Accountability * Integrity * Reliability

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-08-814, a report to the Chairman, Committee on House Administration, House of Representatives

September 2008

ELECTIONS

Federal Program for Certifying Voting Systems Needs to Be Further Defined, Fully Implemented, and Expanded

Why GAO Did This Study

The 2002 Help America Vote Act (HAVA) created the Election Assistance Commission (EAC) and, among other things, assigned the commission responsibility for testing and certifying voting systems. In view of concerns about voting systems and the important role EAC plays in certifying them, GAO was asked to determine whether EAC has (1) defined an effective approach to testing and certifying voting systems, (2) followed its defined approach, and (3) developed an effective mechanism to track problems with certified systems and use the results to improve its approach. To accomplish this, GAO compared EAC guidelines and procedures with applicable statutes, guidance, and best practices, and examined the extent to which they have been implemented.

What GAO Recommends

GAO is making recommendations to EAC relative to establishing and implementing plans to better define and implement its certification program. GAO is also proposing that Congress consider expanding EAC's role under HAVA to include facilitating understanding and resolution of shared problems with noncertified voting systems and providing it with the resources to accomplish this. EAC stated that it generally agrees with GAO's conclusion that its certification program needs to improve and that it accepts GAO's recommendations. It also provided other comments, some of which GAO used to clarify its findings, one recommendation, and its proposal to amend HAVA.

To view the full product, including the scope and methodology, click on GAO-08-814. For more information, contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov.

What GAO Found

EAC has defined an approach to testing and certifying voting systems that follows a range of relevant practices and statutory requirements associated with a product certification program, including those published by U.S. and international standards organizations, and those reflected in HAVA. EAC, however, has yet to define its approach in sufficient detail to ensure that certification activities are performed thoroughly and consistently. This lack of definition also has caused voting system manufacturers and test laboratories to interpret program requirements differently, and the resultant need to reconcile these differences has contributed to delays in certifying systems that several states were intending to use in the 2008 elections. According to EAC officials, these definitional gaps can be attributed to the program's youth and the commission's limited resources being devoted to other priorities. Nevertheless, they said that they intend to address these gaps, but added that they do not yet have written plans for doing so.

EAC has largely followed its defined approach for each of the dozen systems it is in the process of certifying, with one major exception. Specifically, it has not established an effective and efficient repository for certified versions of voting system software, or related procedures and tools, for states and local jurisdictions to use in verifying that their acquired voting systems are identical to what EAC has certified. Further, EAC officials told GAO that they do not have a documented plan or requirements for a permanent solution. As an interim solution, they stated that they will maintain copies of certified versions in file cabinets and mail copies of these versions upon their request by states and local jurisdictions. In GAO's view, this process puts states and local jurisdictions at increased risk of using a version of a system during an election that differs from the certified version.

Under its voting system testing and certification program, EAC has broadly described an approach for tracking problems with certified voting systems and using this information to improve its certification program. While this approach is consistent with some aspects of relevant guidance, key elements are either missing or inadequately defined. According to EAC officials, while they intend to address some of these gaps, they do not have documented plans for doing so. In addition, even if EAC defines and implements an effective approach, it would not affect the vast majority of voting systems that are to be used in the 2008 elections. This is because the commission's approach only applies to those voting systems that it has certified, and it is unlikely that any voting systems will be certified in time to be used in the upcoming elections. Moreover, because most states do not currently require EAC certification for their voting systems, it is uncertain if this situation will change relative to future elections. As a result, states and other election jurisdictions are on their own to discover, disclose, and address any shared problems with these noncertified systems.

Contents

Table

Figures

Abbreviations

EAC	Election Assistance Commission
FEC	Federal Election Commission
HAVA	Help America Vote Act
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
NASED	National Association of State Election Directors
NIST	National Institute of Standards and Technology
NSRL	National Software Reference Library
NVLAP	National Voluntary Laboratory Accreditation Program
VSS	Voting Systems Standards
VSTL	voting system test laboratory
VVSG	Voluntary Voting System Guidelines

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 16, 2008

The Honorable Robert A. Brady
Chairman
Committee on House Administration
House of Representatives

Dear Mr. Chairman:

Following the 2000 and 2004 general elections, we issued a series of reports and testified on virtually every aspect of our nation's election system, including the many challenges and opportunities associated with various types of voting systems.[1] In this regard, we emphasized that the voting systems alone were neither the sole contributor nor solution to the problems that were experienced during the 2000 and 2004 elections, and that the overall election system depended on the effective interplay of people, process, and technology and involved all levels of government. Among other things, we specifically reported in 2001 that no federal entity was responsible for developing voting system standards and for testing and certifying these systems against such standards, and we raised the establishment of such an entity as a matter for congressional consideration.[2]

Subsequently, Congress passed the Help America Vote Act (HAVA), which created the Election Assistance Commission (EAC) and assigned it responsibilities for, among other things, the testing, certification, decertification, and recertification of voting system hardware and software.[3] In 2004, we testified on the challenges facing EAC in meeting its

[1] See, for example, GAO, *Elections: All Levels of Government Are Needed to Address Electronic Voting System Challenges*, GAO-07-576T (Washington, D.C.: Mar. 7, 2007); *Elections: The Nation's Evolving Election System as Reflected in the November 2004 General Election*, GAO-06-450 (Washington, D.C.: June 6, 2006); *Elections: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed*, GAO-05-956 (Washington, D.C.: Sept. 21, 2005); *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).

[2] GAO-02-52.

[3] 42 U.S.C. § 15371.

responsibilities, adding that the commission's ability to meet these challenges depended in part on having adequate resources. In 2007, EAC established and began implementing its voting system certification program. In view of the continuing concerns about voting systems and the important role the commission plays in certifying them, you asked us to determine whether EAC has (1) defined an effective approach to testing and certifying voting systems, (2) followed its defined approach, and (3) developed an effective mechanism to track problems with certified systems and use the results to improve its certification program.

To accomplish this, we reviewed EAC policies, procedures, and standards for testing, certifying, decertifying, and recertifying voting systems and compared them, as appropriate, with applicable statutory requirements and leading practices, such as HAVA and guidance published by the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), and International Electrotechnical Commission (IEC). We also compared EAC actions and artifacts for executing the voting system certification program with its policies, guidelines, and procedures. In addition, we interviewed officials from EAC, NIST, voting system test laboratories (VSTL), voting system manufacturers, and the National Association of State Election Directors (NASED).[4]

We conducted this performance audit at EAC offices in Washington, D.C., from September 2007 to September 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Further details of our objectives, scope, and methodology are included in appendix I.

Results in Brief

EAC has defined an approach to testing and certifying voting systems that follows statutory requirements reflected in HAVA and a range of relevant practices associated with a product certification program, including those

[4] NASED is an independent, nongovernmental organization consisting of state election officials. It voluntarily formed the first national program to test and qualify voting systems to federal standards.

published by U.S. and international standards organizations. In particular, its voting system certification program defines key roles and responsibilities; describes the steps that voting system manufacturers are to follow; provides for testing to be performed by accredited VSTLs; provides for interpretation of voting system standards; includes mechanisms for VSTLs and EAC reviewers to declare their impartiality and independence; and addresses how manufacturer complaints, appeals, and disputes will be handled. Nevertheless, the commission has not developed its approach in sufficient detail to ensure that its certification activities are performed thoroughly and consistently. For example, it has not defined procedures or specific criteria for many of its review activities, including the specific test procedures to be used and how decisions are to be documented. According to EAC officials, these gaps exist because the program is still new and evolving and resources are focused on other commission priorities. Officials further stated that they intend to carry out a number of activities to address these gaps; however, they said that written plans for doing so are not yet developed. Until these definitional gaps are fully addressed, EAC cannot adequately ensure that its certification approach is repeatable and verifiable across all manufacturers and systems. Moreover, these gaps have already led to different interpretations of program requirements among EAC's stakeholders, and the resultant need to reconcile differences has contributed to delays in certifying systems that several states had intended to use in the 2008 elections.

EAC has largely followed its voting system testing and certification approach as defined. For example, it has received and reviewed manufacturer registration applications, system certification applications, and system test plans, as well as issued notices of noncompliance. However, contrary to its own certification program requirements, the commission has yet to establish a sufficient mechanism for states and local jurisdictions to use in verifying that the voting systems that they receive from manufacturers are identical to the ones that were tested and certified. Specifically, EAC has yet to designate a repository of trusted software versions for certified systems, and it has not established plans or time frames for doing so. Instead, EAC officials stated that they plan to store these software builds on compact disks and place the disks in fireproof filing cabinets in their offices, and mail copies of the disks to those states and local jurisdictions that request them, until they can develop a permanent solution. However, the commission has no activities planned or under way to establish one. In addition, EAC has yet to specify exactly what needs to be done to ensure that manufacturers provide effective and efficient tools and processes to support states and local jurisdictions in using the repository to verify that their respective systems match the certified version, and has not developed plans for ensuring that this occurs. Until such tools are in place, state and local election officials are likely to face difficulty in determining whether the systems that they receive from a manufacturer are identical to the system that was tested and certified.

EAC has broadly described an approach to allow it to track and resolve problems with certified voting systems and use the information about these problems to improve its voting system testing and certification program. Under this approach, EAC is to investigate reports alleging defects with certified voting systems, and take action by, for example, issuing a notice of noncompliance, providing the manufacturer with an opportunity to correct the noncompliance, and decertifying a system if the manufacturer does not take sufficient action to bring the system into compliance. In addition, EAC is to periodically inspect the production facilities of voting system manufacturers. However, it has yet to specify how this broadly defined approach will be executed, including what steps will be followed, what criteria will be used to reach decisions, how it will know if system problems have been corrected, and how it will use the information to improve its testing and certification program. In addition, while EAC officials stated that they intend to address some of these gaps, they do not have defined plans or time frames for doing so. According to the EAC officials, this is because the certification program is still new and other priorities have consumed the commission’s limited resources. Until these definitional limitations are addressed, it is unlikely that EAC will be able to effectively track and resolve problems that arise with the systems that it has certified.

Even if EAC defines and implements an effective problem tracking and resolution process for certified systems, these actions will not affect the vast majority of voting systems that are to be used in the 2008 elections, and it is uncertain when this situation will change relative to future elections. This is because of two factors. First, most of the systems to be used will not be systems that were certified by EAC, but instead will be systems that were qualified by the now-discontinued NASED program, or those that were not endorsed by any national entity. Second, HAVA does not explicitly assign EAC any responsibility for non-EAC-certified voting systems, and, according to commission officials, they do not have the authority or resources to identify and address problems with these systems in the same manner that they do for EAC-certified systems. Although EAC has established a mechanism, under its HAVA-required information clearinghouse responsibility, to post state and local officials’ reports of problems and experiences with non-EAC-certified systems on its Web site, this mechanism does not involve any EAC actions to facilitate problem understanding or resolution.

Notwithstanding the EAC's efforts to establish an effective voting systems testing and certification program, more can be done to build on its existing program to be more effective. Accordingly, we are making recommendations to the Chair of the EAC to develop and execute plans to (1) establish detailed procedures, review criteria, and documentation requirements to ensure that voting system testing and certification reviews are conducted thoroughly, consistently, and verifiably; (2) establish an accessible and available software repository for its certified systems, and procedures and review criteria for manufacturer-provided tools for using the repository; and (3) fully define and implement certified voting system problem tracking and resolution activities, and apply lessons learned to improve the program. We are also providing a matter for congressional consideration aimed at expanding EAC's role under HAVA such that, consistent with the nonregulatory and voluntary nature of its certification program, the commission is assigned responsibility for providing resources and services to facilitate understanding and resolution of problems with non-EAC-certified voting systems that will be used in future elections, and provided with the resources needed to accomplish this.

EAC provided written comments on a draft of this report, signed by the EAC Executive Director and reprinted in their entirety in appendix II. In its comments, the commission described our review and report as helpful as it works to fully implement and improve its voting system certification program. It also stated that it agrees with the report's conclusions that more can be done to build on the program and ensure that certifications are based on consistently performed reviews. Further, it stated that it generally accepts our three recommendations, adding that it will work hard to implement them. EAC provided additional comments on the findings that underlie each of the recommendations, which it described as needed to clarify and avoid confusion about some aspects of its certification program. In response to these comments, we have modified the report, as appropriate, to clarify our findings and one of the recommendations.

The commission also provided comments on our matter for congressional consideration, including characterizing it as intending "to affect a sea change in the way that EAC operates its testing and certification" program. We agree that EAC does not have the authority to compel the manufacturers or states and local jurisdictions to submit to its testing and certification program and that the wording of the matter in our draft inadvertently led EAC to believe that our proposal would require the commission to assume a more regulatory role. In response to EAC's comments, and in order to avoid any misunderstanding as to the intent of this matter for congressional consideration, we have modified its wording.

Background

All levels of government share responsibility in the overall U.S. election system. 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.[5] 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 overall U.S. election system 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 decentralize election administration, so that it is 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.[6] Further, these thousands of jurisdictions rely on many different types of voting methods that employ a wide range of voting system makes, models, and versions.

[5] GAO-02-3.

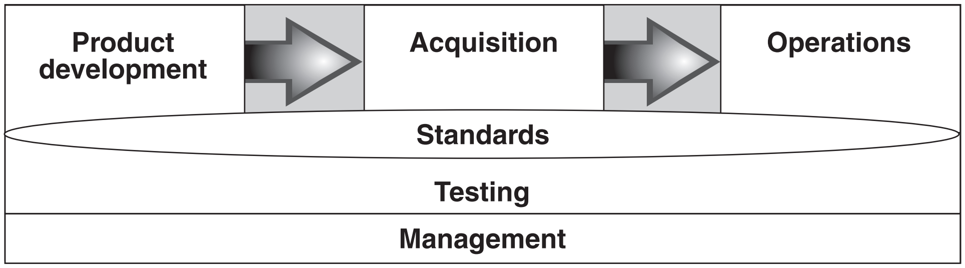
[6] GAO-02-3.

The U.S. Election System Depends on Effective Interactions among People, Processes, and Technology

Voting systems are but one facet of a multifaceted, continuous election system that involves the interplay of people, processes, and technology. All levels of government, as well as commercial voting system manufacturers and VSTLs, play key roles in ensuring that voting systems perform as intended.

Electronic voting systems are typically developed by manufacturers, purchased as commercial off-the-shelf products, and operated by state and local election administrators. These activities can be viewed as three phases in a system's life cycle: product development, acquisition, and operations (see fig. 1). Spanning these life cycle phases are key processes, including managing the interplay of people, processes, and technologies, and testing the systems and components. In addition, voting system standards are important through all of these phases because they provide the criteria for developing, testing, and acquiring the systems, and they specify the necessary documentation for operating the systems. We discuss each of these phases after figure 1.

Figure 1: A Voting System Life Cycle Model



Source: GAO analysis of EAC, NIST, and Institute of Electrical and Electronics Engineers (IEEE) publications.

- The *product development* phase includes such activities 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 manufacturer.

- The *acquisition phase* includes such procurement-related activities as publishing a solicitation, evaluating offers, choosing a voting technology, choosing a vendor, and awarding and administering contracts. Activities in this phase are primarily the responsibility of state and local governments, but include responsibilities that are shared with the vendor, such as establishing contracts.

- *The operations* phase consists of such activities as ballot design and programming, setup of systems before voting, pre-election testing, 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, whose officials may, in turn, rely on or obtain assistance from system vendors for aspects of these activities.

- *Standards* for voting systems were developed at the national level by the Federal Election Commission (FEC) in 1990 and 2002 and were updated by EAC in 2005. Voting system standards serve as guidance for product developers in building systems, a framework for state and local governments to evaluate systems, and as the basis for documentation needed to operate the systems.

- *Testing* processes are conducted throughout the life cycle of a voting system. For example, manufacturers conduct product testing during development of the system. Also, national certification testing of products submitted by system manufacturers is conducted by nationally accredited VSTLs. States and local jurisdictions also perform a range of system tests.

- *Management* processes help to ensure that each life cycle phase produces desirable outcomes. Typical management activities include planning, configuration management, system performance review and evaluation, problem tracking and correction, human capital management, and user training.

Testing and Certification Are Important to Ensuring Voting System Security and Reliability

Testing electronic voting systems for conformance with requirements and standards is critical to ensuring their security and reliability, and an essential means to ensuring that systems perform as intended. In addition, such testing can help find and correct errors in systems before they are used in elections. If done properly, testing provides voters with assurance and confidence that their voting systems will perform as intended.

Testing is particularly important for electronic voting systems because these systems have become our Nation’s predominant method of voting, and concerns have been raised about their security and reliability. As we reported in 2005,[7] these concerns include 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. Further, security experts

[7] GAO-05-956.

and some election officials have expressed concerns that tests performed under the NASED program by independent testing authorities and state and local election officials did not adequately assess voting systems' security and reliability. Consistent with these concerns, most of the security weaknesses that we identified in our prior report[8] related to systems that NASED had previously qualified. Our report also recognized that security experts and others pointed to these weaknesses as an indication that both the standards and the NASED testing program were not rigorous enough with respect to security, and that these concerns were amplified by what some described as a lack of transparency in the testing process.

EAC's Responsibilities under HAVA include Certifying Voting Systems

Enacted in October 2002, HAVA affects nearly every aspect of the election system, from voting technology to provisional ballots and from voter registration to poll worker training.[9] Among other things, the act authorized $3.86 billion in funding over several fiscal years for states to replace punch card and mechanical lever voting equipment, improve election administration and accessibility, and perform research and pilot studies. In addition, the act established EAC and assigned it responsibility for, among other things, (1) updating voting system standards, (2) serving as a clearinghouse for election-related information, (3) accrediting independent test laboratories, and (4) certifying voting systems. EAC began operations in January 2004. In 2004, we testified on the challenges facing EAC in meeting its responsibilities.[10] For example, we reported that EAC needed to move swiftly to strengthen voting system standards and the testing associated with these standards. We also reported that the commission's ability to meet its responsibilities depended, in part, on the adequacy of the resources at its disposal.

Updating standards: HAVA requires EAC to adopt a set of federal voting system standards, referred to as the Voluntary Voting System Guidelines (VVSG). In December 2005, the commission adopted the VVSG, which defines a set of specifications and requirements against which voting systems are to be designed, developed, and tested to ensure that they provide the functionality, accessibility, and security capabilities required

[8] GAO-05-956.

[9] Help America Vote Act, Pub. L. No. 107-252 (Oct. 29, 2002).

[10] GAO-04-975T.

to ensure the integrity of voting systems. As such, the VVSG specifies the functional requirements, performance characteristics, documentation requirements, and test evaluation criteria for the national certification of voting systems. In 2007, the Technical Guidelines Development Committee[11] submitted its recommendations for the next iteration of the VVSG to EAC. The commission has yet to establish a date when the update will be approved and issued.

Serving as an information clearinghouse: HAVA requires EAC to maintain a clearinghouse of information on the experiences of state and local governments relative to, among other things, implementing the VVSG and operating voting systems. As part of this responsibility, EAC posts voting system reports and studies that have been conducted or commissioned by a state or local government on its Web site. These reports must be submitted by a state or local government that certifies that the report reflects its experience in operating a voting system or implementing the VVSG. EAC does not review the information for quality and does not endorse the reports and studies.

Accrediting independent test laboratories: HAVA assigned responsibilities for laboratory accreditation to both EAC and NIST. In general, NIST focuses on assessing laboratory technical qualifications and recommends laboratories to EAC for accreditation. EAC uses NIST's assessment results and recommendations, and augments them with its own review of related laboratory capabilities to reach an accreditation decision. As we have previously reported,[12] EAC and NIST have defined their respective approaches to accrediting laboratories that address relevant HAVA requirements. However, neither approach adequately defines all aspects of an effective program to the degree needed to ensure that laboratories are accredited in a consistent and verifiable manner. Accordingly, we recently made recommendations to NIST and EAC aimed at addressing these limitations.

Certifying voting systems: HAVA requires EAC to provide for the testing, certification, decertification, and recertification of voting system hardware

[11] The Technical Guidelines Development Committee was established under HAVA to assist EAC in developing the VVSG.

[12] GAO, *Elections: Federal Programs for Accrediting Laboratories That Test Voting Systems Need to Be Better Defined and Implemented*, GAO-08-770 (Washington, D.C.: Sept. 9, 2008).

and software. EAC's voting system testing and certification program is described in detail in the following section.

Prior to HAVA, no federal agency was assigned or assumed responsibility for testing and certifying voting systems against the federal standards. Instead, NASED, through its voting systems committee, assumed this responsibility by accrediting independent test authorities, which in turn tested equipment against the standards. When testing was successfully completed, the independent test authorities notified NASED that the equipment satisfied testing requirements. NASED would then qualify the system for use in elections. According to a NASED official, the committee has neither qualified any new or modified systems, nor taken any actions to disqualify noncompliant systems, since the inception of EAC's testing and certification program in January 2007.

Overview of EAC's Voting System Testing and Certification Program

EAC implemented its voting system testing and certification program in January 2007. According to the commission's Testing and Certification Program Manual, EAC certification means that a voting system has been successfully tested by an accredited VSTL, meets requirements set forth in a specific set of federal voting system standards, and performs according to the manufacturer's specifications.

The process of EAC's voting system testing and certification program consists of seven major phases. Key stakeholders that are involved in this process include voting system manufacturers, accredited VSTLs, and state and local election officials. These seven phases are described in the following text and depicted in figure 2.

1. Manufacturer Registration

All manufacturers must be registered to submit a voting system for certification. To register, a manufacturer must provide such information as organizational structure and contact(s); quality assurance, configuration management, and document retention procedures; and identification of all manufacturing and assembly facilities. In registering, the manufacturer agrees to certain duties and requirements at the outset of its participation in the program. These requirements include properly using and representing EAC's certification label, notifying the commission of any changes to a certified system, permitting EAC to verify the manufacturer's quality control procedures by inspecting fielded systems and manufacturing facilities, cooperating with any inquiries and investigations about certified systems, reporting any known malfunction of a system, and otherwise adhering to all procedural requirements of the program manual.

Once a manufacturer submits a completed application form and all required attachments, EAC reviews the submission for sufficiency using a checklist that maps to the application requirements listed in the program manual. If the application passes the review, EAC provides the manufacturer with a unique identification code and posts the applicant as a registered manufacturer on the commission's Web site, along with relevant documentation.

2. Voting System Certification Application

For each voting system that a manufacturer wishes to have certified, it submits an application package. The package includes an application form requiring the following: manufacturer information, accredited VSTL selection, applicable voting system standard(s), nature of submission, system name and version number, all system components and corresponding version numbers, and system configuration information. The package also includes the following documentation: system implementation statement,[13] functional diagram, and system overview. EAC reviews the submission for completeness and accuracy and, if it is acceptable, notifies the manufacturer and assigns a unique application number to the system.

3. Test Plan Development and Approval

Once the certification application is accepted, the accredited VSTL prepares and submits to EAC a test plan defining how it will ensure that the system meets applicable standards and functions as intended. When a laboratory submits its test plan, EAC's technical reviewers assess it for adequacy. If the plan is deemed not acceptable, the commission provides written notice to the laboratory that includes a description of the problems identified and the steps required to remedy the test plan. The laboratory may take remedial action and resubmit the test plan until it is accepted by EAC reviewers.

4. Test Plan Execution

The VSTL executes the approved test plan and notifies EAC directly of any test anomalies or failures, along with any changes or modifications to the test plan as a result of testing. The laboratory then prepares a test results report.

5. Test Report Review

The VSTL submits the test results report to EAC's Program Director who reviews it for completeness. If it is complete, the technical reviewers

[13] The implementation statement provides a summary description of the voting system's capabilities, including identification of voting system hardware and software components, version numbers, and dates. It must also include a checklist identifying all of the VVSG requirements that the voting system implements.

analyze the report in conjunction with related technical documents and the test plan for completeness, appropriateness, and adequacy. The reviewers submit their findings to the Program Director, who either recommends certification of the system to the Decision Authority, EAC's Executive Director, or refers the matter back to the reviewers for additional specified action and resubmission.

6. Initial Certification Decision and Appeal

EAC's Decision Authority reviews the recommendation of the Program Director and supporting materials and issues a written decision to the manufacturer. If certification is denied, the manufacturer may request an opportunity to correct the basis for the denial or may request reconsideration of the decision after submitting supporting written materials, data, and a rationale for its position. The Decision Authority considers the request and issues a written decision. If the decision is to deny certification, the manufacturer may request an appeal in writing to the Program Director. The Appeal Authority, which consists of two or more EAC Commissioners or other individuals appointed by the Commissioners who have not previously served as the initial or reconsideration authority, consider the appeal. The Appeal Authority may overturn the decision if it finds that the manufacturer has demonstrated by clear and convincing evidence that its system met all substantive and procedural requirements for certification.

7. Final Certification

The initial decision becomes final and EAC issues a Certificate of Conformance to the manufacturer, and posts the system on the list of certified voting systems on its Web site, when the manufacturer and VSTL successfully demonstrate that the voting system under test has been:

- *Subject to a trusted build:* The voting system's source code is converted to executable code in the presence of at least one VSTL representative and one manufacturer representative, using security measures to ensure that the executable code is a verifiable and faithful representation of the source code. This demonstrates that (1) the software was built as described in the technical documentation, (2) the tested and approved source code was actually used to build the executable code on the system, and (3) no other elements were introduced in the software build. It also serves to document the configuration of the certified system for future reference.

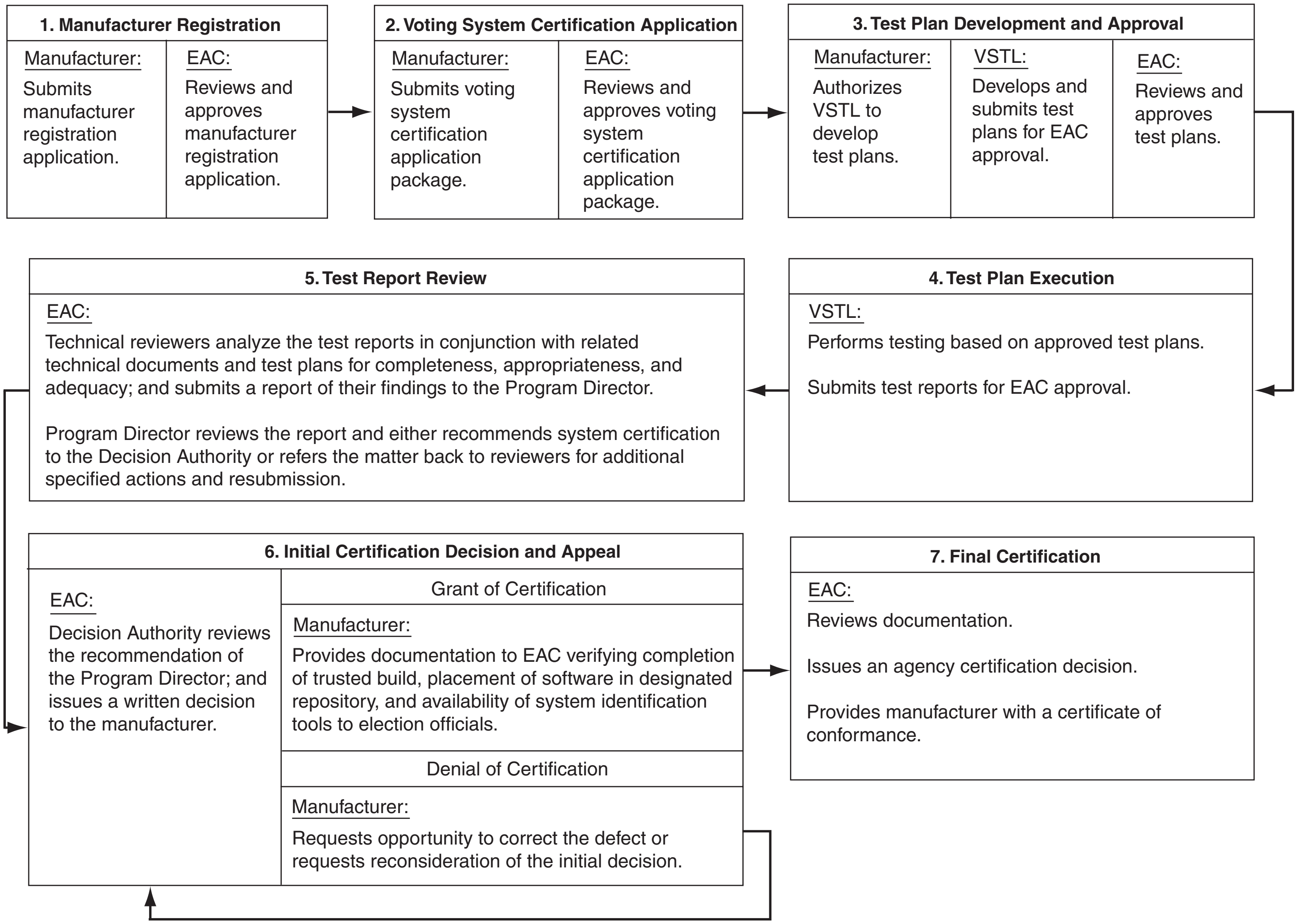
- *Placed in a software repository:* The VSTL delivers the following to one or more trusted repositories designated by EAC: (1) source code used for the trusted build and its file signatures;[14] (2) disk image of the prebuild, build environment, and any file signatures to validate that it is unmodified; (3) disk image of the postbuild, build environment, and any file signatures to validate that it is unmodified; (4) executable code produced by the trusted build and its file signatures of all files produced; and (5) installation device(s) and its file signatures.

- *Verified using system identification tools:* The manufacturer creates and makes available system identification tools that federal, state, and local officials can use to verify that their voting systems are unmodified from the system that was certified. These tools are to provide the means to identify and verify hardware and software.[15]

[14] A signature of a file or set of files is produced using a HASH algorithm. A file signature, sometimes called a HASH value, consists of a value that is computationally infeasible of being produced by two similar but different files. File signatures are used to verify that files are unmodified from their original versions.

[15] Hardware is commonly verified by identifying the model and revision numbers of the system's printed wiring boards and major subunits, and comparing the system with detailed photographs of the printed wiring boards and internal construction of the unit that was tested and approved. Software is typically verified by using a self-booting compact disk or similar device to verify the file signatures of the system application files and of all nonvolatile files that the application files access during operation, and comparing against the file signatures of the original executable files that were placed in the software repository.

Figure 2: EAC Voting System Testing and Certification Process



1. Manufacturer Registration

Manufacturer: Submits manufacturer registration application.

EAC: Reviews and approves manufacturer registration application.

2. Voting System Certification Application

Manufacturer: Submits voting system certification application package.

EAC: Reviews and approves voting system certification application package.

3. Test Plan Development and Approval

Manufacturer: Authorizes VSTL to develop test plans.

VSTL: Develops and submits test plans for EAC approval.

EAC: Reviews and approves test plans.

4. Test Plan Execution

VSTL: Performs testing based on approved test plans.

Submits test reports for EAC approval.

5. Test Report Review

EAC: Technical reviewers analyze the test reports in conjunction with related technical documents and test plans for completeness, appropriateness, and adequacy; and submits a report of their findings to the Program Director.

Program Director reviews the report and either recommends system certification to the Decision Authority or refers the matter back to reviewers for additional specified actions and resubmission.

6. Initial Certification Decision and Appeal

EAC: Decision Authority reviews the recommendation of the Program Director; and issues a written decision to the manufacturer.

Grant of Certification

Manufacturer: Provides documentation to EAC verifying completion of trusted build, placement of software in designated repository, and availability of system identification tools to election officials.

Denial of Certification

Manufacturer: Requests opportunity to correct the defect or requests reconsideration of the initial decision.

7. Final Certification

EAC: Reviews documentation.

Issues an agency certification decision.

Provides manufacturer with a certificate of conformance.

Source: GAO analysis of EAC data.

Note: At the review and approval of manufacturer registration applications, voting system certification applications, and test plans, EAC may request additional clarification or information before approval.

EAC's Approach Largely Follows Many Accepted Practices, but Needs to Be Further Defined

To its credit, EAC has taken steps to develop an approach to testing and certifying voting systems that follows statutory requirements and many recognized and accepted practices. However, the commission has not developed its approach in sufficient detail to ensure that its certification activities are performed thoroughly and consistently. It has not, for example, defined procedures or specific criteria for many of its review activities, and for ensuring that the decisions made, and their basis, are properly documented. According to EAC officials, these gaps exist because the program is still new and evolving and resources are limited. Officials further stated that they do not yet have written plans for addressing these gaps. Until these gaps are addressed, EAC cannot adequately ensure that its approach is repeatable and verifiable across all manufacturers and systems. Moreover, this lack of definition has caused EAC stakeholders to interpret certification requirements differently, and the resultant need to reconcile these differences has contributed to delays in certifying systems that several states were planning on using in the 2008 elections.

EAC's Approach Reflects Key Practices and Statutory Requirements

Product certification or conformance testing is a means by which a third party provides assurance that a product conforms to specific standards. In the voting environment, EAC is the third party that provides assurance to the buyer (e.g., state or local jurisdictions) that the manufacturer's voting system conforms to the federal voting standards set forth in FEC's 2002 Voting System Standards (VSS) or EAC's 2005 VVSG.

Several organizations, such as NIST, ISO, and IEC, have individually or jointly developed guidance for product certification and conformance testing programs.[16] This guidance includes, among other things, (1) defining roles and responsibilities for all parties involved in the certification process, (2) defining a clear and transparent process for applicants to follow, (3) ensuring that persons involved in the process are impartial and independent, (4) establishing a process for handling complaints and appeals, and (5) having testing conducted by competent laboratories. Further, HAVA established statutory requirements for a federal testing and certification program. These requirements include

[16] NIST, *Conformance Testing and Certification Model for Software Specifications*, Lisa Carnahan, Lynne Rosenthal, and Mark Skall, March 1998; and ISO/IEC, Guide 65: 1996 (E) *General Requirement for bodies operating product certification systems*, First Edition; and Guide 60: 2004 (E) *Conformity Assessment - Code of good practice*, Second Edition.

ensuring that the program covers testing, certification, decertification, and recertification of voting system hardware and software.

EAC's defined voting system certification approach reflects these key practices. Specifically:

- EAC has defined the roles and responsibilities for itself, the VSTLs, and manufacturers in its Testing and Certification Program Manual. These roles and responsibilities are described in table 1.

Table 1: EAC Certification Program Roles and Responsibilities

Key players	Roles and responsibilities
EAC	• Establish and maintain the testing and certification program • Be the authority for granting and withdrawing certification • Provide the procedural requirement of the program • Review manufacturer registration applications for sufficiency • Review certification applications for completeness and accuracy • Provide technical guidance • Perform technical reviews of test plans, test reports, and other technical documents • Resolve disputes about voting system standards and program administration
VSTLs	• Prepare test plans and test methodologies • Conduct testing to approved test plans • During testing, report any changes to approved test plans and all test failures or anomalies • Record results of testing in a test report • Meet all requirements of EAC's laboratory accreditation program
Manufacturers	• Provide required information to EAC • Adhere to program requirements • Submit voting system to EAC for certification • Report malfunctions with certified voting systems and submit corrective action plans to address any issues that violate EAC's program

Source: GAO analysis of EAC documentation.

- EAC's testing and certification process is documented in its program manual. Among other things, the manual clearly defines the program's administrative requirements that manufacturers and VSTLs are to follow. EAC has made the program manual, along with supporting policies and clarifications, publicly available on its Web site, and has made program-related news and correspondence publicly accessible as they have come available.

- EAC's certification program addresses impartiality and independence. For example, EAC policy states that all personnel and contractors involved in the certification program are subject to conflict-of-interest reporting and review. In addition, the policy mandates conflict-of-interest and conduct statements for the technical reviewers that support the program, requires conflict-of-interest reporting and reviews to ensure the independence of EAC personnel assigned to the program, and requires that all VSTLs maintain and enforce policies that prevent conflict-of-interest or the appearance of a conflict-of-interest, or other prohibited practices.

- EAC's program manual outlines its process for the resolution of complaints, appeals, and disputes received from manufacturers and laboratories. These can be about matters relating to the certification process, such as test methods, procedures, test results, or program administration. Specifically, the program manual contains policies and procedures for submitting a Request for Interpretation, which is a means by which a registered manufacturer or accredited laboratory seeks clarification on a specific voting system standard, including any misunderstandings or disputes about a standard's interpretation or implementation. The manual also contains policies, requirements, and procedures for a manufacturer to file an appeal on a decision denying certification, request an opportunity to correct a problem, and request reconsideration of a decision. In addition, EAC provides for Notices of Clarification, which offer guidance and explanation on the requirement and procedure of the program. Notices may be issued pursuant to a clarification request from a laboratory or manufacturer. EAC may also issue a notice or interpretation if it determines that any general clarifications are necessary.

- EAC has a VSTL accreditation program. This program is supported by NIST's National Voluntary Laboratory Accreditation Program (NVLAP), which is a long established and recognized laboratory accreditation program. According to EAC's program manual, all certification testing is to be performed by a laboratory accredited by NIST and EAC. Further, all subcontracted testing is to be performed by a laboratory accredited by either NIST or the American Association of Laboratory Accreditation for the specific scope of needed testing. Finally, any prior testing will only be accepted if it was conducted or overseen by an accredited laboratory and was reviewed and approved by EAC.

HAVA also established certain requirements for EAC's voting system testing and certification program.[17] Under HAVA, EAC is to provide for the testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories. EAC's defined approach addresses each of these areas.

According to program officials, EAC's certification program reflects many leading practices because the commission consciously sought out these best practices during program development. Officials stated that their intention is to develop a program that stringently tests voting systems to the applicable standards; therefore, they consulted with experts to assist with drafting the program manual. For example, according to EAC officials, they met with officials from other federal agencies that conduct certification testing in order to benefit from their lessons learned. By reflecting relevant practices, standards, and legislative requirements in its defined approach, EAC has provided an important foundation for having an effective voting system testing and certification program.

EAC's Approach Does Not Sufficiently Define the Details for Certifications to Be Performed Thoroughly and Consistently

EAC has yet to define its approach for testing and certifying electronic voting systems in sufficient detail to ensure that its certification activities are performed thoroughly and consistently. It has not, for example, defined procedures or specific criteria for many of its review activities and for ensuring that the decisions made are properly documented. EAC officials attributed this lack of definition to the fact that the program is still new and evolving, and they stated that available resources are constrained by competing priorities. Until these details are defined, EAC will be challenged to ensure that testing and review activities are repeatable across different systems and manufacturers, and that the activities it performs are verifiable. Moreover, this lack of definition is likely to result in different interpretations of program requirements by stakeholders, which has already resulted in the need to reconcile different interpretations and thereby caused delays in certifying systems that several states intended to use in the 2008 elections. In such cases, the delays are forcing states to either not require EAC certification or rely on an alternative system.

[17] 42 U.S.C. § 15371.

According to federal and international guidance,[18] having well-defined and sufficiently detailed program management controls help to ensure that programs are executed effectively and efficiently. Relative to a testing and certification program, such management controls include, among other things, having (1) defined procedures and established criteria for performing evaluation activities so that they will be performed in a comparable, unambiguous, and repeatable manner for each system and (2) required documentation to demonstrate that procedural evaluation steps and related decisions have been effectively performed, including provisions for review and approval of such documentation by authorized personnel.

EAC's defined approach for voting system testing and certification lacks such detail and definition. With respect to the first management control, the commission has not defined procedures or specific criteria for many of its review activities, instead it relies on the personal judgment of the reviewers. Specifically, the program manual states that EAC, with the assistance of its technical experts, as necessary, will review manufacturer registration applications, system certification applications, test plans, and test reports, but it does not define procedures or criteria for conducting these reviews. For example:

- The program manual states that upon receipt of a completed manufacturer registration application, EAC will review the information for sufficiency. However, it does not define what constitutes sufficiency and what this sufficiency review should entail. Rather, EAC officials said that this is left up to the individual reviewer's judgment.
- The program manual lists the information that manufacturers are required to submit as part of their certification applications and states that EAC will review the submission for completeness and accuracy. While the commission has developed a checklist for determining whether the required information was included in the application, neither the program manual nor the checklist describe how reviewers should perform the review or assess the adequacy of the information provided. For example, EAC requires certification applications to include a functional diagram

[18] NIST, *Conformance Testing and Certification Framework*, Lisa Carnahan, Lynne Rosenthal, and Mark Skall, April 2001; *Conformance Testing*, Martha Gray, Alan Goldfine, Lynne Rosenthal, and Lisa Carnahan; and *Conformance Testing and Certification Model*; and ISO/IEC, Guide 65: 1996 (E); Guide 60: 2004 (E); and Guide 7: 1994 (E) *Guidelines for drafting of standards suitable for use for conformity assessment*, Second Edition.

depicting how the components for the voting system function and interact, as well as a system overview that includes a description of the functional and physical interfaces between components. Although the checklist provides for determining whether these items are part of the application package, it does not, for example, provide for checking them for completeness and consistency. Moreover, we identified issues with completeness and consistency of these documents for approved certification application packages. Again, EAC officials said that these determinations are to be based on each reviewer's judgment.

- The program manual states that test plans are to be reviewed for adequacy. However, it does not define adequacy or how such reviews are to be performed. This lack of detail is particularly problematic because EAC officials told us that the VSS and VVSG contain many vague and undefined requirements. According to these officials, reviewers have been directed to ensure that VSTLs stress voting systems during testing, based on what they believe are the most difficult and stringent conditions likely to be encountered in an election environment that are permissible under the standards.

- The program manual states that EAC technical experts will assess test results reports for completeness, appropriateness, and adequacy. However, it does not define appropriateness and adequacy or the procedural steps for conducting the review.

- The program manual requires VSTLs to use all applicable test suites issued by EAC when developing test plans. However, program officials stated that they currently do not have defined test suites and NIST officials said that they are focused on preparing test suites for the forthcoming version of the VVSG and not the 2005 version. As a result, each laboratory develops its own unique testing approach, which requires each to interpret what is needed to test for compliance with the standards and increases the risk of considerable variability in how testing is performed. To address this void, EAC has tasked NIST with developing test suites for both the 2005 VVSG and the yet-to-be-released update to these guidelines.[19] Until then, EAC officials acknowledge that they will be challenged to ensure that testing conducted on different systems or at different VSTLs is consistent and comparable.

[19] EAC has not yet established a date for finalizing these guidelines.

With respect to the second management control, the commission has not defined the documentation requirements that would demonstrate that procedural steps, evaluations, and related decision making have been performed in a thorough, consistent, and verifiable manner. Specifically, while the program manual requires the Program Director to maintain documentation to demonstrate that procedures and evaluations were effectively performed, EAC has yet to specify the nature or content of this documentation. For example:

- The program manual requires technical reviewers to assess test plans and test reports prepared by laboratories and then to submit reports of their findings to the Program Director. However, EAC does not require documentation of how these reviews were performed beyond completion of a recently developed checklist, and this checklist does not provide for capturing how decisions were reached, including steps performed and criteria applied. For example, the VVSG requires that systems permit authorized access and prevent unauthorized access, and lists examples of measures to accomplish this, such as computer-generated password keys and controlled access security. While the checklist cites this requirement and provides for the reviewer to indicate whether the test plan satisfies it, it does not provide specific guidance on how to determine whether the access control measures are adequate, and it does not provide for documenting how the reviewer made such a decision.
- The program manual does not require supervisory review of work conducted by EAC personnel. Moreover, it does not require that the reviewers be identified.

According to EAC officials, its approach does not yet include such details because it is still new and evolving and because the commission's limited resources have been devoted to other priorities.[20] To address these gaps, EAC officials stated that they intend to undertake a number of activities. For example, the Program Director stated that in the near-term, the technical reviewers will collaborate and share views on each test plan and test report under review as a way to provide consistency, and they will use a recently finalized checklist for test plan and test report reviews. In the longer term, EAC intends to define more detailed procedures for each step in its process. However, it has yet to establish documented plans, including the level of resources needed to accomplish this. Until these

[20] According to the Program Director, the program has requested additional certification resources for fiscal year 2009.

plans are developed and executed, EAC will be challenged to ensure that its testing and certification activities are performed thoroughly and consistently across different systems, manufacturers, and VSTLs.

Moreover, this lack of program definition surrounding certification testing and review requirements has already caused, and could continue to cause, differences in how EAC reviewers, VSTLs, and manufacturers interpret the requirements. For example, the program requires sufficient and adequate testing, but it does not define what constitutes sufficient and adequate. As a result, laboratory officials and manufacturer representatives told us that EAC reviewers have interpreted these requirements more stringently than they have, and that reconciling these different interpretations has already caused delays in the approval of test plans,[21] and they will likely prevent EAC from certifying any systems in time for use in the upcoming 2008 elections. This is especially problematic for those states that have statutory or other requirements to use federally certified systems and that have a need to acquire or upgrade existing systems for these elections. In this regard, 18 states reported to us that they were relying on EAC to certify systems for use in the 2008 elections, but now will have to adopt different strategies for meeting their states' respective EAC certification requirements. For example, officials for several states said that they would use the same system as in 2006, while officials for other states described plans to either undertake upgrades to existing systems without federal certification, or change state requirements to no longer require EAC certification.

[21] In a May 2008 correspondence to state election officials, EAC cited several issues that have contributed to delays in certifying voting systems, such as manufacturers and VSTLs having to adjust to the demands of the commission's program and the lack of standardized test methods.

EAC Has Largely Followed Its Defined Certification Approach, but a Key System Verification Capability to Support States and Local Jurisdictions Is Not Yet in Place

EAC has largely followed its defined certification approach for each of the dozen voting systems that it is in the process of certifying, with one major exception. Specifically, it has not established sufficient means for states and local jurisdictions to verify that the voting systems that each receives from its manufacturer have system configurations that are identical to those of the system that the EAC certified, and it has not established plans or time frames for doing so. This means that states and local jurisdictions are at increased risk of using a version of a system during an election that differs from the certified version. This lack of an effective and efficient verification capability could diminish the value of an EAC system certification.

EAC Has Largely Followed Its Defined Certification Approach

EAC has largely executed its voting system testing and certification program as defined. While no system has yet to complete all major steps of the certification process discussed in the Background section of this report, and thus receive certification, 12 different voting systems have completed at least the first step of the process, and some have completed several steps. Specifically, as of May 2008, EAC had received, reviewed, and approved 12 manufacturer registration applications, and these approved manufacturers have collectively submitted certification applications for 12 different systems, of which EAC has accepted 9. For these 9 systems, manufacturers have submitted 7 test plans, of which EAC has reviewed and approved 2 plans. In 1 of these 2 cases, EAC has received a test results report, which it is currently in the process of reviewing. At the same time, EAC has responded to 8 requests for interpretations of standards from manufacturers and laboratories. EAC has also issued 6 notices of clarification, which provide further guidance and explanation on the program requirements and procedures.

Our analysis of available certification-related documentation showed that in each of the 12 systems submitted for certification, all elements of each executed step in the certification process were followed. With respect to the manufacturer registration step, EAC reviewed and approved all 12 applications, as specified in its program manual. For the certification application step, EAC reviewed and approved 9 applications. In doing so, EAC issued 3 notices of noncompliance to manufacturers for failure to comply with program requirements. In each notice, it identified the area of noncompliance, and described what requested relevant information or corrective action(s) was needed in order to participate in the program. In 1 of the cases, EAC terminated the certification application due to the manufacturer's failure to respond within the established time frame, which is consistent with the program manual. These actions were generally consistent with its program manual.

EAC Has Not Established a Sufficient Means for States and Local Jurisdictions to Verify That Their Systems Match the Certified Version

Notwithstanding EAC's efforts to follow its defined approach, it has not yet established a sufficient mechanism for states and local jurisdictions to use in verifying that the voting systems that they receive from manufacturers for use in elections are identical to the systems that were actually tested and certified. According to EAC's certification program manual, final certification is conditional upon (1) testing laboratories depositing certified voting system software into an EAC-designated repository and (2) manufacturers creating and making available system identification tools for states and local jurisdictions to use in verifying that their respective systems' software configurations match that of the software for the system that was certified and deposited into the repository. However, EAC has yet to establish a designated repository or procedures and review criteria for evaluating the manufacturer-provided tools, and has not established plans or time frames for doing so. While none of the ongoing system certifications have progressed to the point where these aspects of EAC's defined approach is applicable, they will be needed when the first system's test results are approved. Until both aspects are in place, state and local officials will likely face difficulties in determining whether the systems that they receive from manufacturers are the same as the systems that EAC certified.

EAC's program requires the use of a designated software repository for certified voting systems. Specifically, the certification program manual states that final certification will be conditional upon, among other things, the manufacturer and VSTL creating and documenting a trusted software build,[22] and the laboratory depositing the build in a designated repository. In its 2005 VVSG, EAC designated NIST's National Software Reference Library (NSRL) as its repository and required its use. However, program officials stated that the commission does not intend to use the NSRL as its designated repository because the library cannot perform all required

[22] The trusted build produces a file signature of the executable code as well as file signatures of the installation disk(s). A file signature is produced using a HASH algorithm, sometimes called a HASH value, which creates a value that is computationally infeasible of being produced by two similar but different files. These file signatures are deposited into EAC's designated repository. Election jurisdictions can refer to the file signatures of the installation disk(s) to validate the software before installing it on the voting system.

functions. While these officials added that they may use the NSRL for portions of the certification program, they said it will not serve as EAC's main repository.

Nevertheless, the commission has not established plans to identify and designate another repository, and has yet to define minimum requirements (functional, performance, or interface) for what it requires in a repository to efficiently support states and local jurisdictions. As an interim measure, an EAC official stated that they will store the trusted builds on compact disks and keep the disks in fireproof filing cabinets in their offices. According to the official, this approach is consistent with established program requirements because the program manual merely refers to the use of a trusted archive or repository designated by EAC. Under this measure, state and local election officials will have to request physical copies of material from EAC and wait for the materials to be physically packaged and delivered. This interim approach is problematic for several reasons, including the demand for EAC resources to keep up with the requests during a time when the Executive Director told us that a more permanent repository solution has not been a commission focus because its limited resources have been focused on other priorities.

EAC has also not defined how it will ensure that manufacturers develop and provide to states and local jurisdictions tools to verify their respective systems' software against the related trusted software builds.[23] According to the program manual, final certification of a voting system is also conditional upon manufacturers creating and making available to states and local jurisdictions tools to compare their systems' software with the trusted build in the repository. In doing so, the program manual states that manufacturers shall develop and make available tools of their choice, and that the manufacturer must submit a letter certifying the creation of the tools and include a copy and description of the tools to EAC. The commission may choose to review the tools. Further, the 2005 VVSG provides some requirements for software verification tools, for example, that the tools provide a method to comprehensively list all software files that are installed on the voting system. However, EAC has yet to specify exactly what needs to be done to ensure that manufacturers provide

[23] According to Section 7.4.6 of Volume I of the 2005 VVSG, the verification process should be able to be performed using commercial off-the-shelf software and hardware available from sources other than the voting system manufacturer. If such tools are commercially available, then election officials will be able to independently acquire the tools needed to verify that their systems are unmodified.

effective and efficient system identification tools and processes, and it has not developed plans for ensuring that this occurs. Instead, EAC has stated that until it defines procedures to supplement the program manual, it will review each tool submitted. However, the commission has yet to establish specific criteria for the assessment.

Without an established means for effectively and efficiently verifying that acquired systems have the same system configurations as the version that EAC certified, states and local jurisdictions will not know whether they are using federally certified voting systems. The absence of such tools unnecessarily increases the risk of a system bearing EAC's mark of certification differing from the certified version.

EAC's Mechanism for Tracking and Resolving Problems with Certified Voting Systems Lacks Sufficient Definition, and Its Scope Is Limited

As part of its voting system testing and certification program, EAC has broadly described an approach for tracking and resolving problems with certified voting systems, and using the information about these problems to improve its program. This approach reflects some key aspects of relevant guidance. However, other aspects are either missing or not adequately defined, and although EAC officials stated that they intend to address some of these gaps, the commission does not have defined plans or time frames for doing so. Commission officials cited limited resources and competing priorities as reasons for these gaps.

In addition, EAC's problem tracking and resolution approach does not extend to any of the voting systems that are likely to be used in the 2008 elections, and it is uncertain when, and to what extent, this situation will change. This is because its defined scope only includes EAC-certified systems; it does not include NASED-qualified systems or any other systems to be used in elections. EAC officials stated that the reason for this is because HAVA does not explicitly assign the commission responsibility for systems other than those it certifies. This means that no federal entity is currently responsible for tracking and facilitating the resolution of problems found with the vast majority of voting systems that are used across the country today and that could be used in the future, and thus states and local jurisdictions must deal with problems with their systems on their own.

EAC's Approach for Tracking and Resolving Problems with Certified Systems Partially Reflects Relevant Guidance

According to published guidance,[24] tracking and resolving problems with certified products is important. This includes, among other things, (1) withdrawing certification if a product becomes noncompliant; (2) regularly monitoring the continued compliance of products being produced and distributed; (3) investigating the validity and scope of reports of noncompliance; (4) requiring the manufacturer to take corrective actions when defects are discovered, and ensuring that such actions are taken; and (5) using information gathered from these activities to improve the certification program.

EAC's approach for tracking and resolving problems with certified systems reflects some, but not all aspects of these five practices. First, its certification program includes provisions for withdrawing certification for noncompliant voting systems. For example, the program manual describes procedures for decertifying a noncompliant voting system if the manufacturer does not take timely or sufficient action to correct instances of noncompliance. According to these procedures, the decertification decision cannot be made until the manufacturer is formally alerted to the noncompliance issue and provided with an opportunity to correct the issue (problem) or to submit additional information for consideration. Also, a manufacturer can dispute the decision by requesting an appeal. The procedures also state that upon decertification, the manufacturer cannot represent the system as certified and the system may not be labeled with a mark of certification. In addition, EAC is to remove the system from its list of certified systems, alert state and local election officials to the system's decertification via monthly newsletters and e-mail updates, and post all correspondence regarding the decertification on its Web site.

Second, EAC's certification program includes provisions for postcertification oversight of voting systems and manufacturers. Specifically, the program manual provides for reviewing and retesting certified voting systems to ensure that they have not been modified, and that they continue to comply with applicable standards and program requirements. In addition, the program manual calls for periodic

[24] ISO/IEC, Guide 65: 1996 (E); Guide 67: 2004 (E) *Conformity assessment – Fundamentals of product certification*, First Edition; Guide 28: 1982 (E) *General rules for a model third-party certification system for products*, First Edition; and Guide 53: 2005 (E) *Conformity assessment – Guidance on the use of an organization's quality management system in product certification*, Second Edition; and ISO, Guide 27: 1983 (E) *Guidelines for corrective action to be taken by a certification body in the event of misuse of its mark of conformity*, First Edition.

inspections of manufacturers' facilities to evaluate their production quality, internal test procedures, and overall compliance with program requirements. However, the program manual states that reviewing and retesting of certified systems is an optional step, and does not specify the conditions under which this option is to be exercised. Further, while the program manual provides for conducting periodic inspections of manufacturers' facilities, it does not define, for example, who is to conduct the inspections, what procedures and evaluation criteria are to be used in conducting them, and how they are to be documented.

Third, EAC's certification program includes provisions for investigating reports of system defects. According to the program manual, investigations of reports alleging defects with certified systems begin as informal inquiries that can potentially become formal investigations. Specifically, the Program Director is to conduct an informal inquiry in which a determination is made regarding whether the reported defect information is both credible and deserving of system decertification if found to be credible. If both conditions are met, then a formal investigation is to be conducted. Depending on the outcome, decertification of the system could result. However, the program manual does not call for assessing the scope or impact of any defects identified, such as whether a defect is confined to an individual unit or whether it applies to all such units. Further, the program manual does not include procedures or criteria for determining the credibility of reported defects, or any other aspect of the inquiry or investigation, such as how EAC will gain access to systems once they are purchased and fielded by states and local jurisdictions. This is particularly important because EAC does not have regulatory authority over state election authorities, and thus, it cannot compel their cooperation during an inquiry or investigation.

Fourth, EAC's certification program does not address how it will verify that manufacturers take required corrective actions to fix problems identified with certified systems. Specifically, the program manual states that the manufacturer is to provide EAC with a compliance plan describing how it will address identified defects. However, the program manual does not define an approach for evaluating the compliance plan and confirming that a manufacturer actually implements the plan. According to EAC officials, they see their role as certifying a system and informing states of modifications. As a result, they do not intend to monitor how or whether manufacturers implement changes to fielded systems. In their view, the state ultimately decides if a system will be fielded.

Fifth, EAC's certification program provides for using information generated by its problem tracking and resolution activities to improve the program. According to the program manual, information gathered during quality monitoring activities will be used to, among other things, identify improvements to the certification process and to inform the related standards-setting process. Further, the program manual states that information gathered from these activities will be used to inform relevant stakeholders of issues associated with operating a voting system in a real-world environment and to share information with jurisdictions that use similar systems. However, the program manual does not describe how EAC will compile and analyze the information gathered to improve the program, or how it will coordinate these functions with information gathered in performing its HAVA-assigned clearinghouse function.[25]

EAC officials attributed the state of their problem tracking and resolution approach to the newness of the certification program and the fact that the commission's limited resources have been devoted to other priorities. In addition, while these officials said that they intend to address some of these gaps, they do not have defined plans or time frames for doing so. For example, while EAC officials stated that they plan to develop procedures for investigating voting system problems and for inspecting manufacturing facilities, they said that it is the states' responsibility to ensure that corrective actions are implemented on fielded systems. To illustrate their resource challenges, these officials told us that three staff are assigned to the testing and certification program and each is also supporting other programs.[26] In addition, they said that the commission's technical reviewers are experts who, under Office of Personnel Management regulation, work no more than one-half of the time of the year.[27]

[25] EAC is responsible for, among other things, serving as a national clearinghouse and resource for the compilation of information by, for example, carrying out duties related to the testing, certification, decertification, and recertification of voting system hardware and software. 42 U.S.C. § 15322.

[26] For fiscal year 2009, EAC requested $16,679,000 in appropriated funds for salaries and expenses. Of this amount, $4,202,000 was for personnel compensation providing for 37 full-time-equivalent (FTE) EAC staff salaries. The 37 FTEs include 29 full-time-permanent employees and 8 experts, consultants, contract employees, students, and other part-time employees.

[27] According to 5 C.F.R. § 304.103(c)(2)(i), an agency may reappoint an expert or consultant, with no limit on the number of reappointments, as long as the individual is paid for no more than 6 months of work in a service year.

Given that EAC has not yet certified a system, the impact of these definitional limitations has yet to be realized. Nevertheless, with 12 systems currently undergoing certification, it is important for the commission to address them quickly. If it does not, EAC will be challenged in its ability to effectively track and resolve problems with the systems that it certifies.

EAC's Problem Tracking and Resolution Efforts Do Not Include Most Voting Systems to Be Used in Elections

The scope of EAC's efforts to track and resolve problems with certified voting systems does not extend to those systems that were either qualified by NASED or were not endorsed by any national authority. According to program officials, the commission does not have the authority or the resources needed to undertake such a responsibility. Instead of tracking and resolving problems with these systems, EAC anticipates that they will eventually be replaced or upgraded with certified systems. Our review of HAVA confirmed that the act does not explicitly assign EAC any responsibilities for noncertified systems, although it also does not preclude EAC from tracking and facilitating the resolution of problems with these systems.

As a result, the commission's efforts to track and resolve problems with voting systems do not include most of the voting systems that will be used in the 2008 elections. More specifically, while EAC has efforts under way relative to the certification of 12 voting systems, as we have previously described in this report, commission officials stated that it will be difficult to field any system that EAC anticipates certifying before 2008 in time for the 2008 elections. Thus, voting systems used in national elections will likely be either those qualified under the now-discontinued NASED program, or those not endorsed by any national entity. Moreover, this will continue to be the case until states voluntarily begin to adopt EAC-certified systems, which is currently unclear and uncertain because only 18 states reported having requirements to use EAC-certified voting systems. Restated, most states' voting systems will not be covered by EAC's problem tracking and resolution efforts, and when and if they will is not known. Moreover, manufacturers may or may not upgrade existing, noncertified systems, and they may or may not seek EAC certification of those systems. Thus, it is likely that many states, and their millions of voters, will not use EAC-certified voting systems for the foreseeable future.

Nevertheless, EAC has initiated efforts under the auspices of its HAVA-assigned clearinghouse responsibility[28] to receive information that is volunteered by states and local jurisdictions on problems and experiences with systems that it has not certified, and to post this information on the commission's Web site to inform other states and jurisdictions about the problems. In doing so, EAC's Web site states that the commission does not review the information for quality and does not endorse the reports and studies. Notwithstanding this clearinghouse activity, this means that no national entity is currently responsible for tracking and facilitating the resolution of problems found with the vast majority of voting systems that are in use across the country. This in turn leaves state and local jurisdictions on their own to discover, disclose, and address any shared problems with systems. While this increases the chances of states and local jurisdictions duplicating efforts to get problems fixed, it also increases the chances that problems addressed by one state or jurisdiction may not even be known to another. A key to overcoming this situation will be strong central leadership.

Conclusions

The effectiveness of our nation's overall election system depends on many interrelated and interdependent variables. Among these are the security and reliability of the voting systems that are used to cast and count votes, which in turn depend largely on the effectiveness with which these systems are tested and certified. EAC plays a pivotal role in testing and certifying voting systems. To its credit, EAC has recently established and begun implementing a voting system testing and certification program that is to both improve the quality of voting systems in use across the country, and help foster public confidence in the electoral process. While EAC has made important progress in defining and executing its program, more can be done. Specifically, key elements of its defined approach, such as the extent to which certification activities are to be documented, are vague, while other elements are wholly undefined—such as threshold criteria for making certification-related decisions. Moreover, a key element that is defined—namely, giving states and local jurisdictions an effective and efficient means to access the certified version of a given voting system software—has yet to be implemented. While EAC acknowledges the need to address these gaps, it has yet to develop specific plans or time frames

[28] According to HAVA, EAC shall serve as a national clearinghouse and resource for the compilation of information, including information on the experiences of state and local governments in, for example, operating voting systems.

for completing them that, among other things, ensure that adequate resources for accomplishing them are sought.

Addressing these gaps is very important because their existence not only increases the chances of testing and certification activities being performed in a manner that is neither repeatable nor verifiable, they also can create misunderstanding among manufacturers and VSTLs that can lead to delays in the time needed to certify systems. Such delays have already been experienced, to the point that needed upgrades to current systems will likely not be fielded in time for use in the 2008 elections. Such situations ultimately detract from, and do not enhance, election integrity and voter confidence. Moreover, by not having established an effective means for states and local jurisdictions to verify that the systems each acquires are the same as the EAC-certified version, EAC is increasing the risk of noncertified versions ultimately getting used in an election.

Beyond the state of EAC's efforts to define and follow an approach to testing and certifying voting systems, including efforts to track and resolve problems with certified systems and use this information to improve the commission's testing and certification program, a void exists relative to having a national focus on tracking and resolving problems with voting systems that EAC has not certified, and thus has not been assigned explicit responsibility or has the resources to address. Unless this void is filled, state and local governments will likely continue to be on their own for resolving performance and maintenance issues for the vast majority of voting systems in use today and the near future.

Recommendations for Executive Action

To assist EAC in building upon and evolving its voting systems testing and certification program, we recommend that the Chair of the EAC direct the commission's Executive Director to ensure that plans are prepared, approved, and implemented for developing and implementing

- detailed procedures, review criteria, and documentation requirements to ensure that voting system testing and certification review activities are conducted thoroughly, consistently, and verifiably;

- an accessible and available software repository for testing laboratories to deposit certified versions of voting system software, as well as procedures and review criteria for evaluating related manufacturer-provided tools to support stakeholders in comparing their systems with this repository; and

- detailed procedures, review criteria, and documentation requirements to ensure that problems with certified voting systems are effectively tracked and resolved, and that the lessons learned are effectively used to improve the certification program.

Matter for Congressional Consideration

To address the potentially longstanding void in centrally facilitated problem identification and resolution for non-EAC-certified voting systems, we are raising for congressional consideration expanding EAC's role under HAVA such that, consistent with both the commission's nonregulatory mission and the voluntary nature of its voting system standards and certification program, EAC is assigned responsibility for providing resources and services to facilitate understanding and resolution of common voting system problems that are not otherwise covered under EAC's certification program, and providing EAC with the resources needed to accomplish this.

Agency Comments and Our Evaluation

In written comments on a draft of this report, signed by the EAC Executive Director, and reprinted in appendix II, the commission stated that it agrees with the report's conclusion that more can be done to build on the existing voting system certification program and ensure that certifications are based on consistently performed reviews. In addition, EAC stated that it has found our review and report helpful in its efforts to fully implement and improve this program. It also stated that it generally accepts our three recommendations with little comment, adding that it will work hard to implement them. In this regard, it cited efforts that are planned or underway to address the recommendations.

EAC provided additional comments on the findings that underlie each of the recommendations, which it described as needed to clarify and avoid confusion about some aspects of its certification program. According to EAC, these comments are intended to allay some of the concerns raised in our findings. We summarize and evaluate these comments below, and to avoid any misunderstanding of our findings and the recommendation associated with one of them, we have modified the report, as appropriate, in response to EAC's comments.

EAC also provided comments on our matter for congressional consideration, including characterizing it as intending "to affect a sea change in the way that EAC operates its testing and certification" program. We agree that EAC does not have the authority to compel manufacturers or states and local jurisdictions to submit to its testing and certification program and that the wording of the matter in our draft inadvertently led EAC to believe that our proposal would require the commission to assume a more regulatory role. In response, we have modified the wording that we used to clarify any misunderstanding as to our intent.

With respect to our first recommendation for developing and implementing plans for ensuring that voting system testing and certification review activities are governed by detailed procedures, criteria, and documentation requirements, EAC stated that it is committed to having a program that is rigorous and thorough, and that its program manual creates such a program. It also stated that it agrees with our recommendation and that it will work to further the process in its manual by implementing detailed procedures. In this regard, however, it took issue with five aspects of our finding.

- With respect to our point that criteria and procedures have not been adequately defined for reviewing the information in the manufacturer registration application package, EAC stated that such criteria are not necessary because the package does not require a determination of sufficiency. We do not agree. According to section 2.4.2 of the program manual, EAC is to review completed registration applications for sufficiency. However, as our report states, the manual does not define criteria as to what constitutes sufficiency and what this sufficiency review should entail, and EAC officials stated this determination is left up to the individual reviewer's judgment.
- Concerning our point that criteria and procedures have not been adequately defined for reviewing the information in the system certification application package, EAC stated that a technical review of the package is not required. Rather, it said that the package simply requires a determination that all necessary information is present, adding that it has a checklist to assist a reviewer in determining this. We do not agree with this comment for two reasons. First, our report does not state that the package review is technical in nature, but rather is a review to determine a package's completeness and accuracy. Second, the checklist does not include any criteria upon which to base a completeness and accuracy determination. As EAC's comments confirm, this is important because the information in the package is to be used by technical reviewers as they review test plans and test reports to ensure that the testing covers all aspects of the voting system. For example, EAC requires certification applications to include a functional diagram depicting how the components for the voting system function and interact, as well as a system overview that includes a description of the functional and physical interfaces between components. Although the checklist provides for

determining whether these items are part of the application package, it does not provide for checking them for completeness and consistency. We have clarified this finding in our report by including this example.

- As to our point that EAC has not defined how technical reviewers are to determine the adequacy of system test plans and reports, the commission stated that our report does not take into account what it described as a certification requirements traceability matrix that its technical reviewers use to assess the completeness and adequacy of the plans and reports. However, EAC also acknowledged in its comments that procedures have yet to be established relative to the use of the matrix. Further, we reviewed this matrix, which we refer to in our report as a checklist, and as we state in our report, this checklist does not provide for capturing how decisions were reached, including steps performed and criteria applied. For example, the VVSG requires that systems permit authorized access and prevent unauthorized access, and lists examples of measures to accomplish this, such as computer-generated password keys and controlled access security. While the checklist cites this requirement and provides for the reviewer to indicate whether the test plan satisfies it, it does not provide specific guidance on how to determine whether the access control measures are adequate, and it does not provide for documenting how the reviewer made such a decision. In response to EAC's comments, we have added this access control example to clarify our finding.

- With regard to our point that the program manual does not include defined test suites, EAC commented on the purpose of these test suites and stated that it would not be appropriate to include them in the manual because the manual is not intended to define technical requirements for testing. We agree that the program manual should not include actual test suites, and it was not our intent to suggest that it should. Rather our point is that test suites do not yet exist. Accordingly, we have modified our report to more clearly reflect this. In addition, we acknowledge EAC's comment that NIST is currently in the process of developing test suites, and that it recently sent several test suites to the VSTLs and other stakeholders for review. However, as we state in our report, NIST officials said that they are focused on preparing test suites for the yet-to-be-released update to the VVSG and not the 2005 version. Further, EAC has not yet established plans or time frames for finalizing test suites for either versions of these guidelines, and the program manual does not make reference to the development of these test suites.

- In commenting on our point that differences in interpretation of program requirements have resulted in test plan and report approval delays, EAC stated that its interpretation process provides a means for VSTLs and manufacturers to request clarification of the voting system standards that are ambiguous. We agree with this statement. However, we also believe that having the kind of defined procedures and established criteria that are embodied in our recommendation will provide a common understanding among EAC stakeholders around testing and certification expectations, which should minimize the need to reconcile differences in interpretations later in the process.

With respect to our second recommendation for developing and implementing plans for an accessible and available software repository for certified versions of voting system software, as well as the related manufacturer-provided procedures and tools to support stakeholders in using this repository, EAC stated that it agrees that implementation of a repository is needed. However, it stated that there is some misunderstanding regarding the purpose of the repository and the creation of software identification tools. Specifically, the commission stated that the repository is intended for the commission's own use when conducting investigations of fielded systems, while the manufacturer-provided system identification tools are for use by state and local election officials to confirm that their systems are the same as the one certified by EAC. In addition, it described steps taken or under way to ensure that a repository and identification tools are in place when needed. This includes "placing the onus" on system manufacturers to create verification tools, investigating software storage options, and discussing with another government agency and outside vendors the possibility of providing secure storage for certified software.

We agree with EAC that its repository serves as a tool for its internal use. However, the repository is also to serve state and local election officials in verifying that their respective systems are identical to the EAC-certified versions of the systems. According to the 2005 VVSG software distribution and setup validation requirements, the process for voting system purchasers in verifying that the version of the software that they receive from a manufacturer is the same as the version certified by EAC is to be performed by comparing it with the reference information generated by the designated repository. Further, commission officials told us that EAC's repository needs to be accessible and easy to use by state and local election officials. While we understand that the manufacturer-provided system identification tools serve a separate function from the repository, both tools together are required for state and local election officials to verify their systems. We also acknowledge that the commission has initiated steps relative to establishing a repository and identification tools.

However, our point is that EAC does not have any plans or time frames for accomplishing this. Further, while we agree that the manufacturers are responsible for creating the identification tools, as we stated in our report, EAC has not defined how it will evaluate the manufacturer-provided tools. To avoid any misunderstanding as to these points, we have slightly modified our finding and related recommendation.

Concerning our third recommendation for developing and implementing detailed procedures, review criteria, and documentation requirements for tracking and resolving problems with certified voting systems and applying lessons learned to improve the certification program, EAC stated that the report does not correctly represent its role in confirming that manufacturers actually correct anomalies in all fielded systems, and it added that the commission does not have the authority or the human capital to do so. Accordingly, EAC stated that it informs affected jurisdictions of system changes, but that it is at the discretion of the states and local jurisdictions, and beyond the scope of the commission, to determine whether fixes are made to individual systems in the field.

We agree that the states and local jurisdictions have the responsibility and authority to determine whether they will implement EAC-approved fixes in the systems that they own. However, as we state in our report, published ISO guidance on tracking and resolving problems with certified products recognizes the importance of the certification body's decision to require manufacturers to take corrective actions when defects are discovered, and to ensure that such actions are taken. Although this guidance acknowledges the difficulty in ensuring corrective actions are implemented on all affected units, it states that products should be corrected "to the maximum degree feasible." Given EAC's authority over registered manufacturers, it can play a larger role in ensuring that problems with fielded system are in fact resolved, while maintaining the voluntary nature of its program, by monitoring the manufacturers' efforts to fix systems for those jurisdictions that choose to implement such corrections, and holding manufacturers accountable for doing so. To avoid any confusion about this point, we have slightly modified our finding.

As to our matter for congressional consideration to amend HAVA to give EAC certain additional responsibilities relative to problem resolution on voting systems not certified by EAC, the commission voiced several concerns. Among other things, it stated that our proposal would "affect a sea change in the way that EAC operates its testing and certification" program, changing it from voluntary to mandatory. Further, it stated that it would, in effect, place EAC in a position to act in a regulatory capacity without having the specific authority to do so, as it would necessitate making both the voluntary voting system guidelines and the testing and certification program mandatory for all states. It also stated that it would require EAC to have specific authority to compel manufacturers of these noncertified voting systems to submit their systems for testing, and to compel states and local jurisdictions to report and resolve any identified system problems.

We recognize that both the voting system guidelines and the testing and certification program are voluntary, and that EAC does not have the authority to compel manufacturers or states and local jurisdictions to submit to its testing and certification program, or to force them to correct any known problems or report future problems. We further acknowledge that the wording of the matter for congressional consideration in our draft report resulted in EAC interpreting accomplishment of it as requiring such unintended measures. Therefore, we have modified it to clarify our intent and to avoid any possible misunderstanding. In doing so, we have emphasized our intent for EAC to continue to serve its existing role as a facilitator and provider of resources and services to assist states and local jurisdictions in understanding shared problems, as well as the voluntary nature of both the system guidelines and the testing and certification program. Further, we seek to capitalize on EAC's unique role as a national coordination entity to address a potentially longstanding, situational awareness void as it pertains to voting systems in use in our nation's elections. As we state in our report, this void increases the chances of states and local jurisdictions duplicating efforts to fix common system problems, and of problems addressed by one state or local jurisdiction being unknown to others. We believe that a key to overcoming this will be strong central leadership, and that with the appropriate resources, EAC is in the best position to serve this role.

We are sending a copy of this report to the Ranking Member of the House Committee on House Administration, the Chairman and Ranking Member of the Senate Committee on Rules and Administration, the Chairmen and Ranking Members of the Subcommittees on Financial Services and General Government, Senate and House Committees on Appropriations, and the Chairman and Ranking Member of the House Committee on Oversight and Government Reform. We are also sending copies to the Chair and Executive Director of the EAC, the Secretary of Commerce, the Acting Director of the NIST, and other interested parties. We will also make copies available to others on request. In addition, this report will be available at no charge on the GAO Web site at www.gao.gov.

Should you or your staff have any questions on matters discussed in this report, please contact me at (202) 512-3439 or at hiter@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix III.

Sincerely yours,

Randolph C. Hite

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

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine whether the Election Assistance Commission (EAC) has (1) defined an effective approach to testing and certifying voting systems, (2) followed its defined approach, and (3) developed an effective mechanism to track problems with certified systems and use the results to improve its certification program.

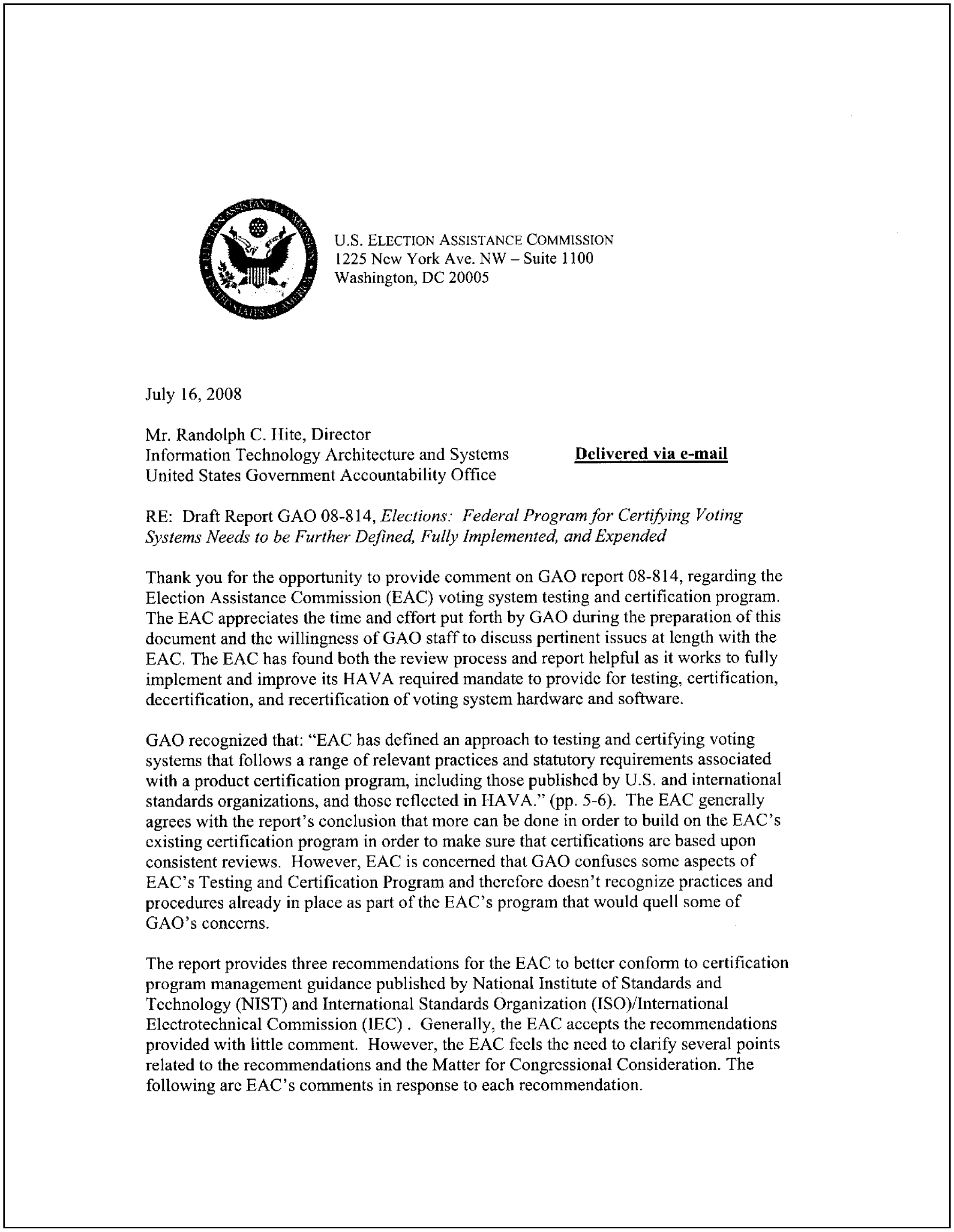
To address the first and third objectives, we researched leading practices relevant to certification testing/conformity assessment and tracking and resolving problems with certified products, including published guidance from the National Institute of Standards and Technology (NIST), International Organization for Standardization, and International Electrotechnical Commission, and legal requirements in the Help America Vote Act. We obtained and reviewed relevant EAC policies and procedures for testing, certifying, decertifying, and recertifying voting systems. Specifically, we reviewed the EAC Certification Program Manual and other EAC-provided documents. We interviewed EAC officials and their technical reviewers, NIST officials, representatives from the industry trade association for voting system manufacturers, representatives from the voting system test laboratories, and the National Association of State Election Directors' point-of-contact for qualified systems. We then compared this body of evidence with the leading practices and related guidance we had researched, as well as applicable legal requirements, to determine whether EAC's program had been effectively defined. In addition, for the third objective, we reviewed the contents and policy of EAC's clearinghouse.

To address our second objective, we obtained and reviewed actions and artifacts from EAC's execution of its certification program to date. We assessed this information against the policies, procedures, and standards outlined in the EAC Certification Program Manual and the 2005 Voluntary Voting System Guidelines, and after discussing and confirming our findings with EAC officials, we determined whether EAC had followed its defined approach.

In addition, to determine the impact of federal certification time frames, we included a question about EAC certification on a survey of officials from all 50 states, the District of Columbia, and 4 territories. We also contacted officials from states that indicated their intent to use EAC certification for the 2008 elections to better understand how they plan to address voting system certification in their state relative to EAC's program. To develop our survey, we reviewed related previous and ongoing GAO work, and developed a questionnaire in collaboration with GAO's survey and subject matter experts. We conducted pretests in person and by telephone with election officials from 5 states to refine and clarify our questions. Our Web-based survey was conducted from December 2007 through April 2008. We received responses from 47 states, the District of Columbia, and all 4 territories (a 95 percent response rate). Differences in the interpretation of our questions among election officials, the sources of information available to respondents, and the types of people who do not respond may have introduced unwanted variability in the responses. We examined the survey results and performed analyses to identify inconsistencies and other indications of error, which were reviewed by an independent analyst. We also contacted officials from those states whose survey response indicated their intent to use EAC certification for the 2008 elections to identify their plans and approaches for state certification in the event that federal certification could not be completed to meet their election preparation schedules.

We conducted this performance audit at EAC offices in Washington, D.C., from September 2007 to September 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Election Assistance Commission



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

July 16, 2008

Mr. Randolph C. Hite, Director
Information Technology Architecture and Systems
United States Government Accountability Office

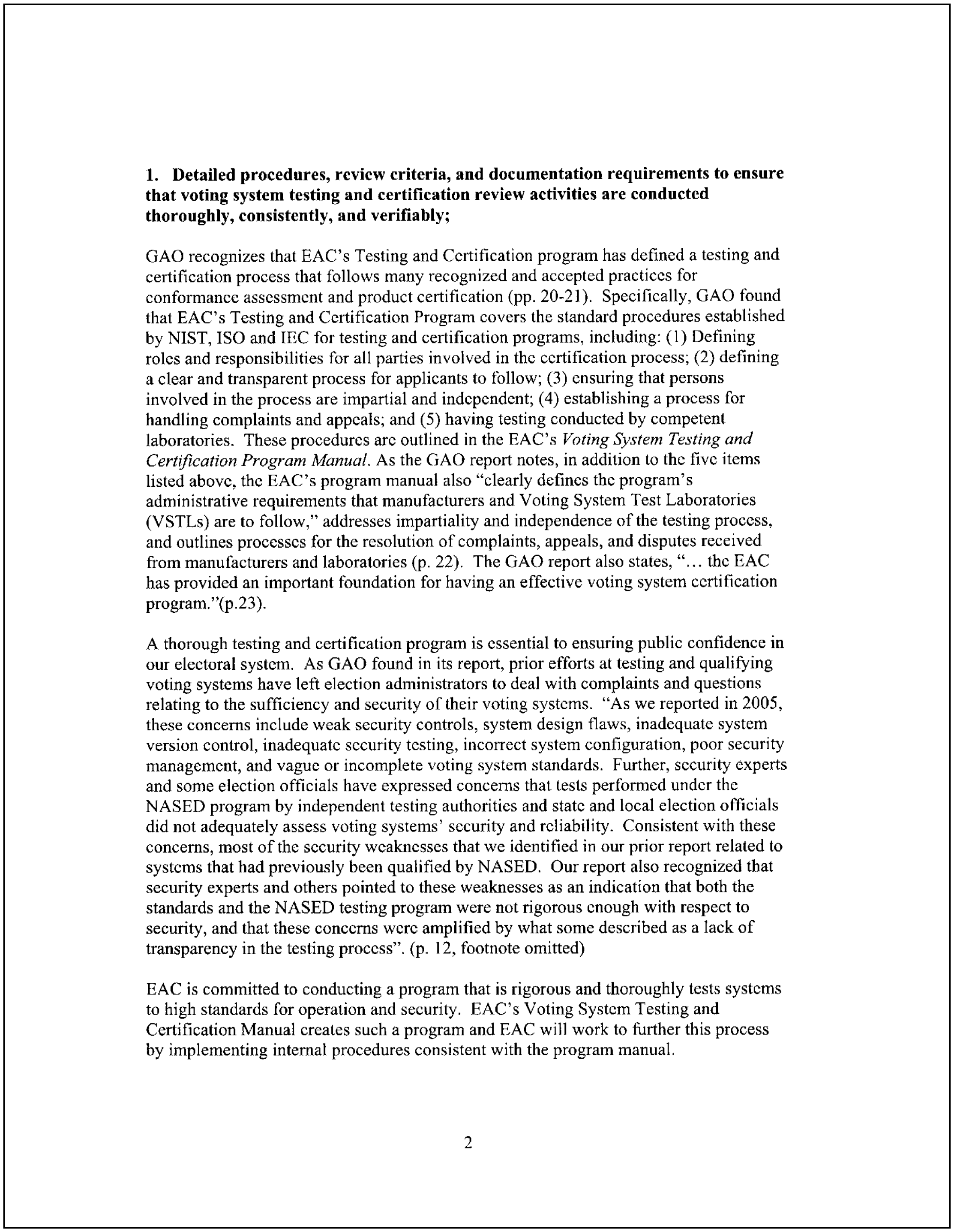
Delivered via e-mail

RE: Draft Report GAO 08-814, *Elections: Federal Program for Certifying Voting Systems Needs to be Further Defined, Fully Implemented, and Expended*

Thank you for the opportunity to provide comment on GAO report 08-814, regarding the Election Assistance Commission (EAC) voting system testing and certification program. 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. The EAC has found both the review process and report helpful as it works to fully implement and improve its HAVA required mandate to provide for testing, certification, decertification, and recertification of voting system hardware and software.

GAO recognized that: "EAC has defined an approach to testing and certifying voting systems that follows a range of relevant practices and statutory requirements associated with a product certification program, including those published by U.S. and international standards organizations, and those reflected in HAVA." (pp. 5-6). The EAC generally agrees with the report's conclusion that more can be done in order to build on the EAC's existing certification program in order to make sure that certifications are based upon consistent reviews. However, EAC is concerned that GAO confuses some aspects of EAC's Testing and Certification Program and therefore doesn't recognize practices and procedures already in place as part of the EAC's program that would quell some of GAO's concerns.

The report provides three recommendations for the EAC to better conform to certification program management guidance published by National Institute of Standards and Technology (NIST) and International Standards Organization (ISO)/International Electrotechnical Commission (IEC) . Generally, the EAC accepts the recommendations provided with little comment. However, the EAC feels the need to clarify several points related to the recommendations and the Matter for Congressional Consideration. The following are EAC's comments in response to each recommendation.



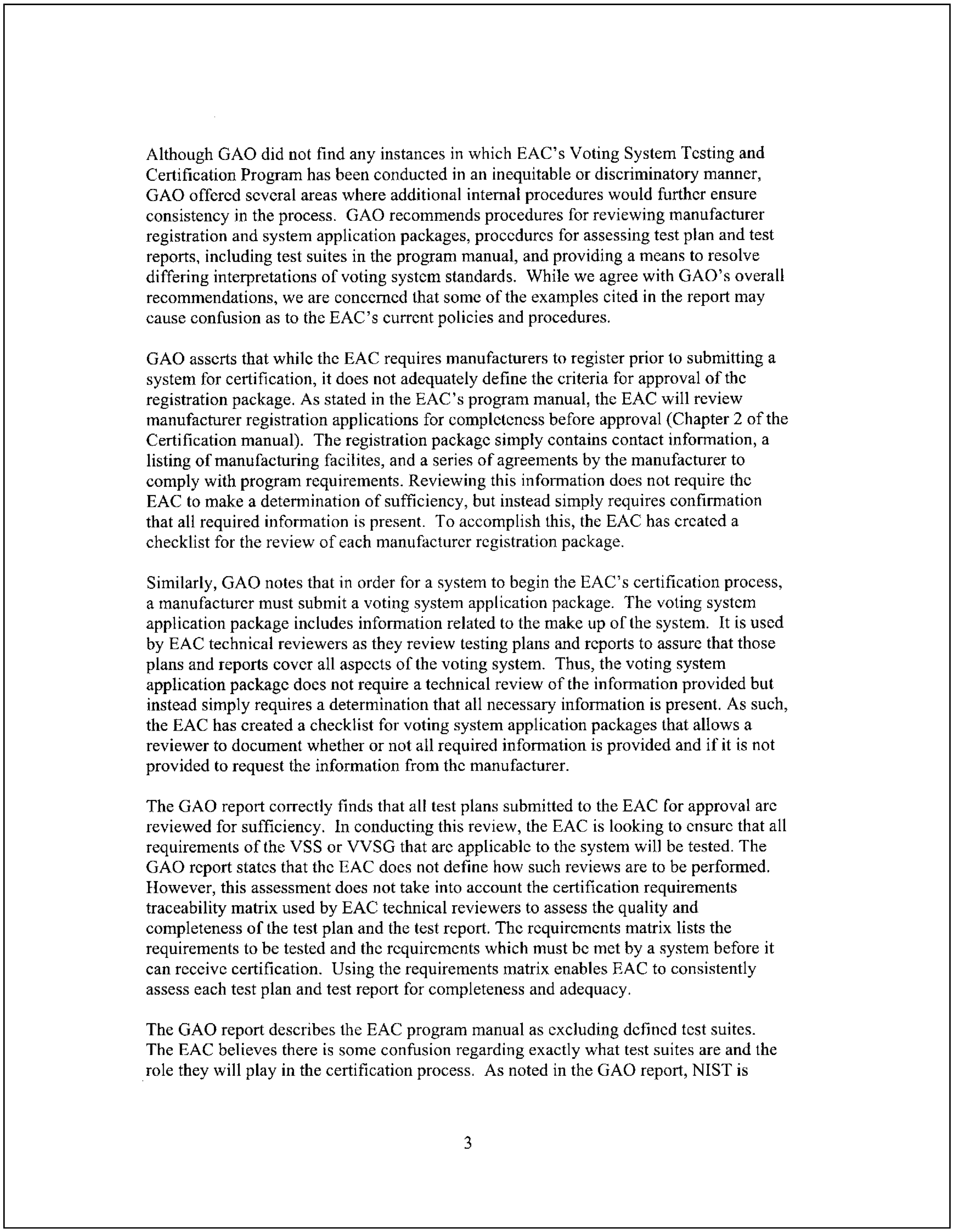
1. Detailed procedures, review criteria, and documentation requirements to ensure that voting system testing and certification review activities are conducted thoroughly, consistently, and verifiably;

GAO recognizes that EAC's Testing and Certification program has defined a testing and certification process that follows many recognized and accepted practices for conformance assessment and product certification (pp. 20-21). Specifically, GAO found that EAC's Testing and Certification Program covers the standard procedures established by NIST, ISO and IEC for testing and certification programs, including: (1) Defining roles and responsibilities for all parties involved in the certification process; (2) defining a clear and transparent process for applicants to follow; (3) ensuring that persons involved in the process are impartial and independent; (4) establishing a process for handling complaints and appeals; and (5) having testing conducted by competent laboratories. These procedures are outlined in the EAC's *Voting System Testing and Certification Program Manual.* As the GAO report notes, in addition to the five items listed above, the EAC's program manual also "clearly defines the program's administrative requirements that manufacturers and Voting System Test Laboratories (VSTLs) are to follow," addresses impartiality and independence of the testing process, and outlines processes for the resolution of complaints, appeals, and disputes received from manufacturers and laboratories (p. 22). The GAO report also states, "... the EAC has provided an important foundation for having an effective voting system certification program."(p.23).

A thorough testing and certification program is essential to ensuring public confidence in our electoral system. As GAO found in its report, prior efforts at testing and qualifying voting systems have left election administrators to deal with complaints and questions relating to the sufficiency and security of their voting systems. "As we reported in 2005, these concerns include 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. Further, security experts and some election officials have expressed concerns that tests performed under the NASED program by independent testing authorities and state and local election officials did not adequately assess voting systems' security and reliability. Consistent with these concerns, most of the security weaknesses that we identified in our prior report related to systems that had previously been qualified by NASED. Our report also recognized that security experts and others pointed to these weaknesses as an indication that both the standards and the NASED testing program were not rigorous enough with respect to security, and that these concerns were amplified by what some described as a lack of transparency in the testing process". (p. 12, footnote omitted)

EAC is committed to conducting a program that is rigorous and thoroughly tests systems to high standards for operation and security. EAC's Voting System Testing and Certification Manual creates such a program and EAC will work to further this process by implementing internal procedures consistent with the program manual.

2



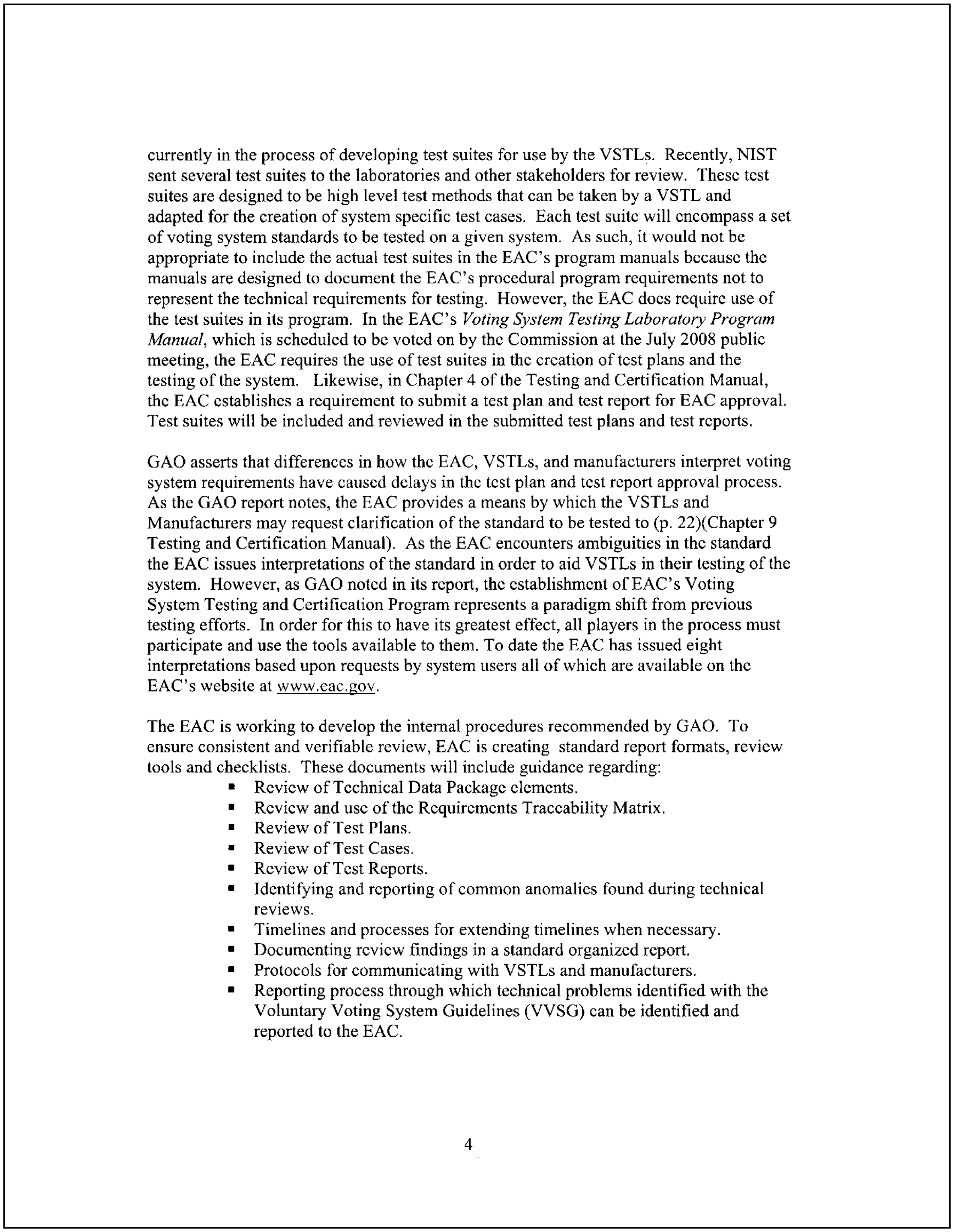
Although GAO did not find any instances in which EAC's Voting System Testing and Certification Program has been conducted in an inequitable or discriminatory manner, GAO offered several areas where additional internal procedures would further ensure consistency in the process. GAO recommends procedures for reviewing manufacturer registration and system application packages, procedures for assessing test plan and test reports, including test suites in the program manual, and providing a means to resolve differing interpretations of voting system standards. While we agree with GAO's overall recommendations, we are concerned that some of the examples cited in the report may cause confusion as to the EAC's current policies and procedures.

GAO asserts that while the EAC requires manufacturers to register prior to submitting a system for certification, it does not adequately define the criteria for approval of the registration package. As stated in the EAC's program manual, the EAC will review manufacturer registration applications for completeness before approval (Chapter 2 of the Certification manual). The registration package simply contains contact information, a listing of manufacturing facilites, and a series of agreements by the manufacturer to comply with program requirements. Reviewing this information does not require the EAC to make a determination of sufficiency, but instead simply requires confirmation that all required information is present. To accomplish this, the EAC has created a checklist for the review of each manufacturer registration package.

Similarly, GAO notes that in order for a system to begin the EAC's certification process, a manufacturer must submit a voting system application package. The voting system application package includes information related to the make up of the system. It is used by EAC technical reviewers as they review testing plans and reports to assure that those plans and reports cover all aspects of the voting system. Thus, the voting system application package does not require a technical review of the information provided but instead simply requires a determination that all necessary information is present. As such, the EAC has created a checklist for voting system application packages that allows a reviewer to document whether or not all required information is provided and if it is not provided to request the information from the manufacturer.

The GAO report correctly finds that all test plans submitted to the EAC for approval are reviewed for sufficiency. In conducting this review, the EAC is looking to ensure that all requirements of the VSS or VVSG that are applicable to the system will be tested. The GAO report states that the EAC does not define how such reviews are to be performed. However, this assessment does not take into account the certification requirements traceability matrix used by EAC technical reviewers to assess the quality and completeness of the test plan and the test report. The requirements matrix lists the requirements to be tested and the requirements which must be met by a system before it can receive certification. Using the requirements matrix enables EAC to consistently assess each test plan and test report for completeness and adequacy.

The GAO report describes the EAC program manual as excluding defined test suites. The EAC believes there is some confusion regarding exactly what test suites are and the role they will play in the certification process. As noted in the GAO report, NIST is

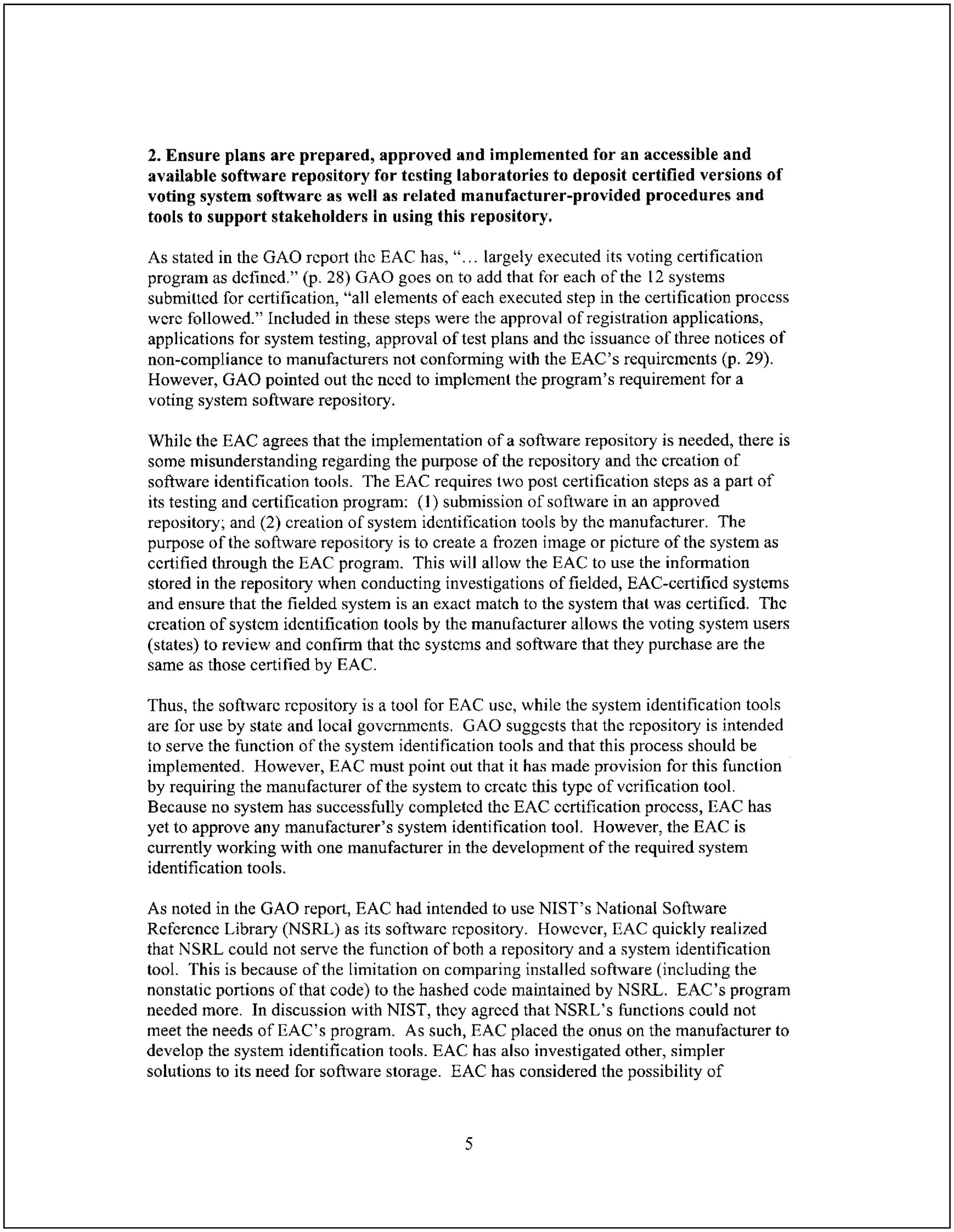


currently in the process of developing test suites for use by the VSTLs. Recently, NIST sent several test suites to the laboratories and other stakeholders for review. These test suites are designed to be high level test methods that can be taken by a VSTL and adapted for the creation of system specific test cases. Each test suite will encompass a set of voting system standards to be tested on a given system. As such, it would not be appropriate to include the actual test suites in the EAC's program manuals because the manuals are designed to document the EAC's procedural program requirements not to represent the technical requirements for testing. However, the EAC does require use of the test suites in its program. In the EAC's *Voting System Testing Laboratory Program Manual*, which is scheduled to be voted on by the Commission at the July 2008 public meeting, the EAC requires the use of test suites in the creation of test plans and the testing of the system. Likewise, in Chapter 4 of the Testing and Certification Manual, the EAC establishes a requirement to submit a test plan and test report for EAC approval. Test suites will be included and reviewed in the submitted test plans and test reports.

GAO asserts that differences in how the EAC, VSTLs, and manufacturers interpret voting system requirements have caused delays in the test plan and test report approval process. As the GAO report notes, the EAC provides a means by which the VSTLs and Manufacturers may request clarification of the standard to be tested to (p. 22)(Chapter 9 Testing and Certification Manual). As the EAC encounters ambiguities in the standard the EAC issues interpretations of the standard in order to aid VSTLs in their testing of the system. However, as GAO noted in its report, the establishment of EAC's Voting System Testing and Certification Program represents a paradigm shift from previous testing efforts. In order for this to have its greatest effect, all players in the process must participate and use the tools available to them. To date the EAC has issued eight interpretations based upon requests by system users all of which are available on the EAC's website at www.eac.gov.

The EAC is working to develop the internal procedures recommended by GAO. To ensure consistent and verifiable review, EAC is creating standard report formats, review tools and checklists. These documents will include guidance regarding:

- Review of Technical Data Package elements.
- Review and use of the Requirements Traceability Matrix.
- Review of Test Plans.
- Review of Test Cases.
- Review of Test Reports.
- Identifying and reporting of common anomalies found during technical reviews.
- Timelines and processes for extending timelines when necessary.
- Documenting review findings in a standard organized report.
- Protocols for communicating with VSTLs and manufacturers.
- Reporting process through which technical problems identified with the Voluntary Voting System Guidelines (VVSG) can be identified and reported to the EAC.



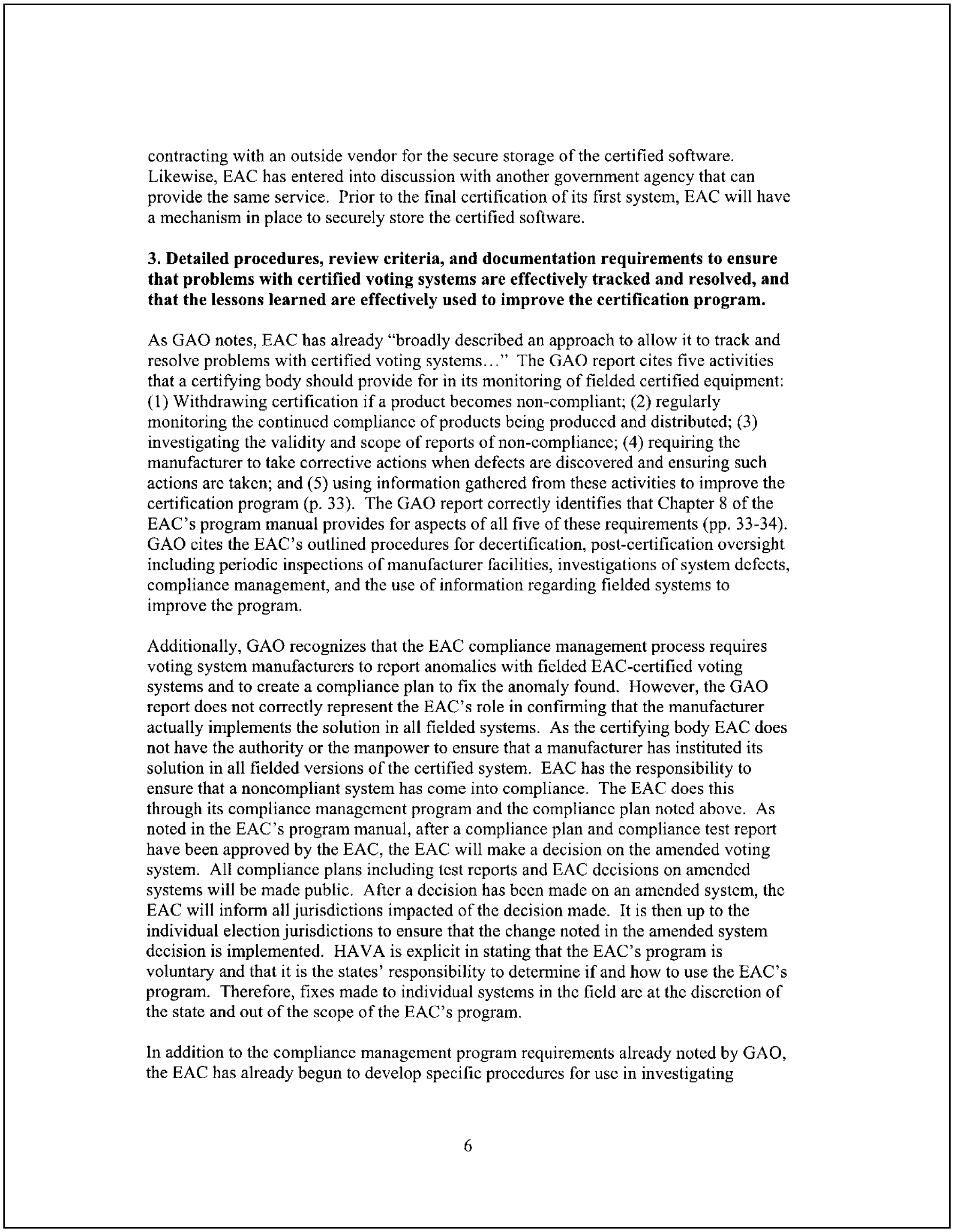
2. Ensure plans are prepared, approved and implemented for an accessible and available software repository for testing laboratories to deposit certified versions of voting system software as well as related manufacturer-provided procedures and tools to support stakeholders in using this repository.

As stated in the GAO report the EAC has, "… largely executed its voting certification program as defined." (p. 28) GAO goes on to add that for each of the 12 systems submitted for certification, "all elements of each executed step in the certification process were followed." Included in these steps were the approval of registration applications, applications for system testing, approval of test plans and the issuance of three notices of non-compliance to manufacturers not conforming with the EAC's requirements (p. 29). However, GAO pointed out the need to implement the program's requirement for a voting system software repository.

While the EAC agrees that the implementation of a software repository is needed, there is some misunderstanding regarding the purpose of the repository and the creation of software identification tools. The EAC requires two post certification steps as a part of its testing and certification program: (1) submission of software in an approved repository; and (2) creation of system identification tools by the manufacturer. The purpose of the software repository is to create a frozen image or picture of the system as certified through the EAC program. This will allow the EAC to use the information stored in the repository when conducting investigations of fielded, EAC-certified systems and ensure that the fielded system is an exact match to the system that was certified. The creation of system identification tools by the manufacturer allows the voting system users (states) to review and confirm that the systems and software that they purchase are the same as those certified by EAC.

Thus, the software repository is a tool for EAC use, while the system identification tools are for use by state and local governments. GAO suggests that the repository is intended to serve the function of the system identification tools and that this process should be implemented. However, EAC must point out that it has made provision for this function by requiring the manufacturer of the system to create this type of verification tool. Because no system has successfully completed the EAC certification process, EAC has yet to approve any manufacturer's system identification tool. However, the EAC is currently working with one manufacturer in the development of the required system identification tools.

As noted in the GAO report, EAC had intended to use NIST's National Software Reference Library (NSRL) as its software repository. However, EAC quickly realized that NSRL could not serve the function of both a repository and a system identification tool. This is because of the limitation on comparing installed software (including the nonstatic portions of that code) to the hashed code maintained by NSRL. EAC's program needed more. In discussion with NIST, they agreed that NSRL's functions could not meet the needs of EAC's program. As such, EAC placed the onus on the manufacturer to develop the system identification tools. EAC has also investigated other, simpler solutions to its need for software storage. EAC has considered the possibility of



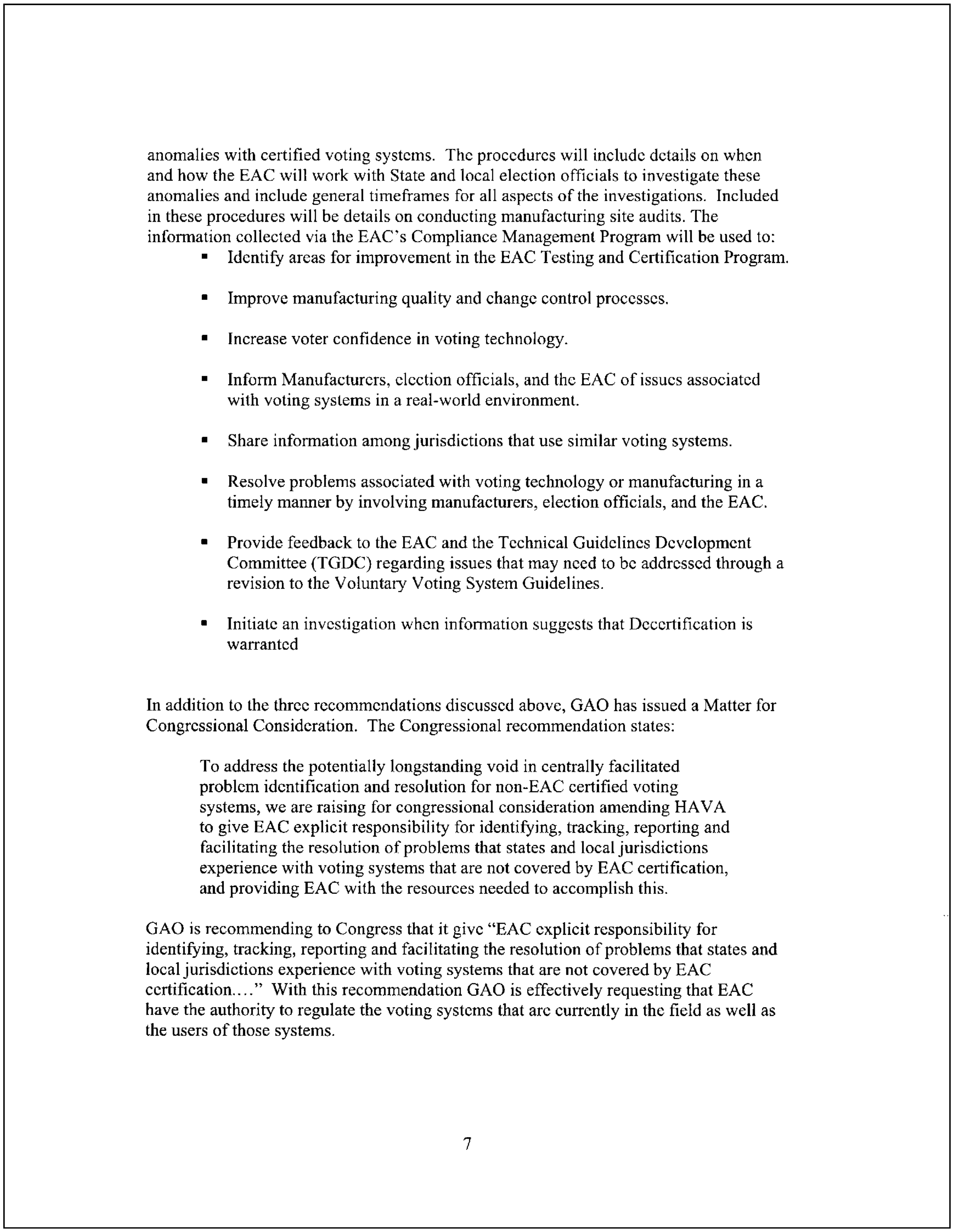
contracting with an outside vendor for the secure storage of the certified software. Likewise, EAC has entered into discussion with another government agency that can provide the same service. Prior to the final certification of its first system, EAC will have a mechanism in place to securely store the certified software.

3. Detailed procedures, review criteria, and documentation requirements to ensure that problems with certified voting systems are effectively tracked and resolved, and that the lessons learned are effectively used to improve the certification program.

As GAO notes, EAC has already "broadly described an approach to allow it to track and resolve problems with certified voting systems…" The GAO report cites five activities that a certifying body should provide for in its monitoring of fielded certified equipment: (1) Withdrawing certification if a product becomes non-compliant; (2) regularly monitoring the continued compliance of products being produced and distributed; (3) investigating the validity and scope of reports of non-compliance; (4) requiring the manufacturer to take corrective actions when defects are discovered and ensuring such actions are taken; and (5) using information gathered from these activities to improve the certification program (p. 33). The GAO report correctly identifies that Chapter 8 of the EAC's program manual provides for aspects of all five of these requirements (pp. 33-34). GAO cites the EAC's outlined procedures for decertification, post-certification oversight including periodic inspections of manufacturer facilities, investigations of system defects, compliance management, and the use of information regarding fielded systems to improve the program.

Additionally, GAO recognizes that the EAC compliance management process requires voting system manufacturers to report anomalies with fielded EAC-certified voting systems and to create a compliance plan to fix the anomaly found. However, the GAO report does not correctly represent the EAC's role in confirming that the manufacturer actually implements the solution in all fielded systems. As the certifying body EAC does not have the authority or the manpower to ensure that a manufacturer has instituted its solution in all fielded versions of the certified system. EAC has the responsibility to ensure that a noncompliant system has come into compliance. The EAC does this through its compliance management program and the compliance plan noted above. As noted in the EAC's program manual, after a compliance plan and compliance test report have been approved by the EAC, the EAC will make a decision on the amended voting system. All compliance plans including test reports and EAC decisions on amended systems will be made public. After a decision has been made on an amended system, the EAC will inform all jurisdictions impacted of the decision made. It is then up to the individual election jurisdictions to ensure that the change noted in the amended system decision is implemented. HAVA is explicit in stating that the EAC's program is voluntary and that it is the states' responsibility to determine if and how to use the EAC's program. Therefore, fixes made to individual systems in the field are at the discretion of the state and out of the scope of the EAC's program.

In addition to the compliance management program requirements already noted by GAO, the EAC has already begun to develop specific procedures for use in investigating



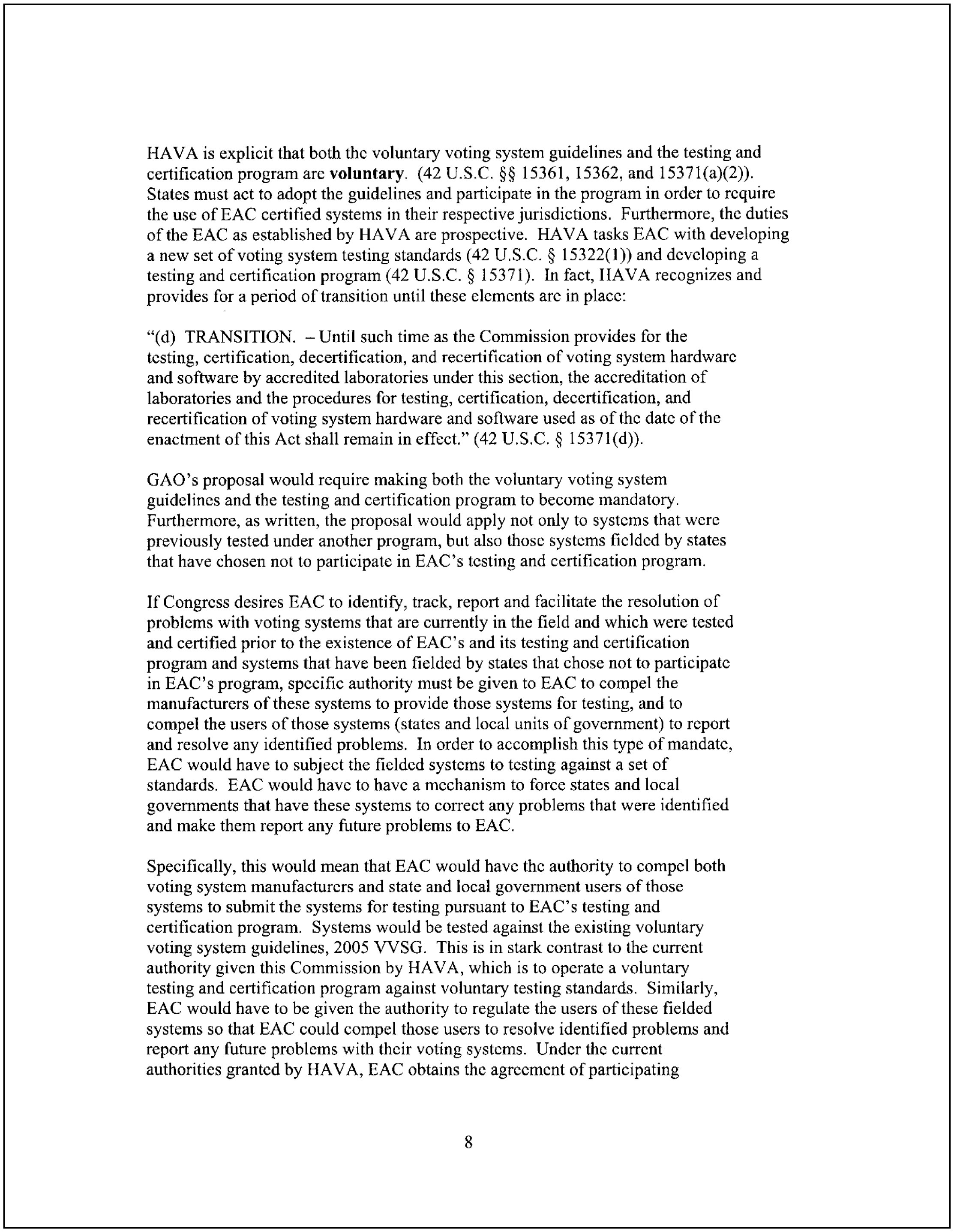
anomalies with certified voting systems. The procedures will include details on when and how the EAC will work with State and local election officials to investigate these anomalies and include general timeframes for all aspects of the investigations. Included in these procedures will be details on conducting manufacturing site audits. The information collected via the EAC's Compliance Management Program will be used to:

- Identify areas for improvement in the EAC Testing and Certification Program.
- Improve manufacturing quality and change control processes.
- Increase voter confidence in voting technology.
- Inform Manufacturers, election officials, and the EAC of issues associated with voting systems in a real-world environment.
- Share information among jurisdictions that use similar voting systems.
- Resolve problems associated with voting technology or manufacturing in a timely manner by involving manufacturers, election officials, and the EAC.
- Provide feedback to the EAC and the Technical Guidelines Development Committee (TGDC) regarding issues that may need to be addressed through a revision to the Voluntary Voting System Guidelines.
- Initiate an investigation when information suggests that Decertification is warranted

In addition to the three recommendations discussed above, GAO has issued a Matter for Congressional Consideration. The Congressional recommendation states:

> To address the potentially longstanding void in centrally facilitated problem identification and resolution for non-EAC certified voting systems, we are raising for congressional consideration amending HAVA to give EAC explicit responsibility for identifying, tracking, reporting and facilitating the resolution of problems that states and local jurisdictions experience with voting systems that are not covered by EAC certification, and providing EAC with the resources needed to accomplish this.

GAO is recommending to Congress that it give "EAC explicit responsibility for identifying, tracking, reporting and facilitating the resolution of problems that states and local jurisdictions experience with voting systems that are not covered by EAC certification...." With this recommendation GAO is effectively requesting that EAC have the authority to regulate the voting systems that are currently in the field as well as the users of those systems.



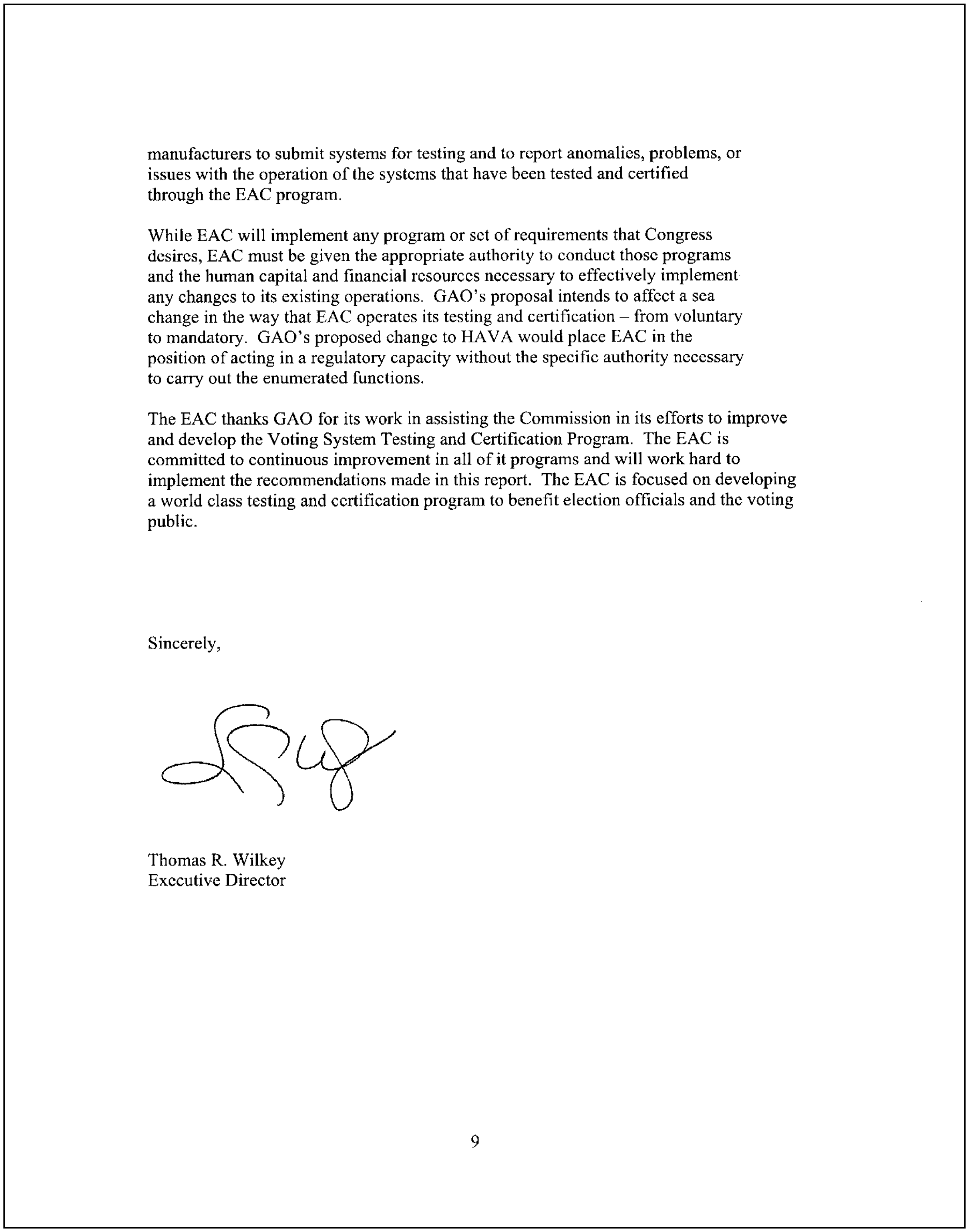
HAVA is explicit that both the voluntary voting system guidelines and the testing and certification program are **voluntary**. (42 U.S.C. §§ 15361, 15362, and 15371(a)(2)). States must act to adopt the guidelines and participate in the program in order to require the use of EAC certified systems in their respective jurisdictions. Furthermore, the duties of the EAC as established by HAVA are prospective. HAVA tasks EAC with developing a new set of voting system testing standards (42 U.S.C. § 15322(1)) and developing a testing and certification program (42 U.S.C. § 15371). In fact, HAVA recognizes and provides for a period of transition until these elements are in place:

"(d) TRANSITION. – Until such time as the Commission provides for the testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories under this section, the accreditation of laboratories and the procedures for testing, certification, decertification, and recertification of voting system hardware and software used as of the date of the enactment of this Act shall remain in effect." (42 U.S.C. § 15371(d)).

GAO's proposal would require making both the voluntary voting system guidelines and the testing and certification program to become mandatory. Furthermore, as written, the proposal would apply not only to systems that were previously tested under another program, but also those systems fielded by states that have chosen not to participate in EAC's testing and certification program.

If Congress desires EAC to identify, track, report and facilitate the resolution of problems with voting systems that are currently in the field and which were tested and certified prior to the existence of EAC's and its testing and certification program and systems that have been fielded by states that chose not to participate in EAC's program, specific authority must be given to EAC to compel the manufacturers of these systems to provide those systems for testing, and to compel the users of those systems (states and local units of government) to report and resolve any identified problems. In order to accomplish this type of mandate, EAC would have to subject the fielded systems to testing against a set of standards. EAC would have to have a mechanism to force states and local governments that have these systems to correct any problems that were identified and make them report any future problems to EAC.

Specifically, this would mean that EAC would have the authority to compel both voting system manufacturers and state and local government users of those systems to submit the systems for testing pursuant to EAC's testing and certification program. Systems would be tested against the existing voluntary voting system guidelines, 2005 VVSG. This is in stark contrast to the current authority given this Commission by HAVA, which is to operate a voluntary testing and certification program against voluntary testing standards. Similarly, EAC would have to be given the authority to regulate the users of these fielded systems so that EAC could compel those users to resolve identified problems and report any future problems with their voting systems. Under the current authorities granted by HAVA, EAC obtains the agreement of participating



manufacturers to submit systems for testing and to report anomalies, problems, or issues with the operation of the systems that have been tested and certified through the EAC program.

While EAC will implement any program or set of requirements that Congress desires, EAC must be given the appropriate authority to conduct those programs and the human capital and financial resources necessary to effectively implement any changes to its existing operations. GAO's proposal intends to affect a sea change in the way that EAC operates its testing and certification – from voluntary to mandatory. GAO's proposed change to HAVA would place EAC in the position of acting in a regulatory capacity without the specific authority necessary to carry out the enumerated functions.

The EAC thanks GAO for its work in assisting the Commission in its efforts to improve and develop the Voting System Testing and Certification Program. The EAC is committed to continuous improvement in all of it programs and will work hard to implement the recommendations made in this report. The EAC is focused on developing a world class testing and certification program to benefit election officials and the voting public.

Sincerely,

Thomas R. Wilkey
Executive Director

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Randolph C. Hite, (202) 512-3439 or hiter@gao.gov

Staff Acknowledgments

In addition to the person named above, Paula Moore, Assistant Director; Mathew Bader; Neil Doherty; Nancy Glover; Dan Gordon; David Hinchman; Valerie Hopkins; Rebecca LaPaze; Jeanne Sung; and Shawn Ward made key contributions to this report.

(310653)

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 "E-mail 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, DC 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

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

PRINTED ON RECYCLED PAPER