July 16, 2008

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

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

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.

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 initial 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