

# The Election Center

an international service association of election and voter registration officials

12543 Westella, Suite 100 Houston, TX 77077 281-293-0101 FAX: 281-293-0453 or 293-8739

Please call us at the main number if you encounter difficulty with either line or E-Mail: [electioncent@pdq.net](mailto:electioncent@pdq.net)

WEBSITE: [www.electioncenter.org](http://www.electioncenter.org)

11-14-2005 Member Alert

**Doug's Note to Members:** Remember when reading this summary (as prepared by Heidi Freier in our office) that the GAO did this study rather quickly and did not have enough time or staff to see the full range of security preparations done by many elections offices around the nation. Some of the recommendations you read here will make you go "Duh!" It would be easy for us to disregard some of the conclusions drawn because they are so basic and are, in fact, some of the very things that significant portions of the elections community already do. And, in some cases, the GAO seems to place more credibility in the critics positions and statements than those of elections professionals. The wisest course of action for election officials, in my mind, is to take the criticisms to heart, recheck every security procedure, place higher emphasis on security issues, and, if necessary, do "overkill" in assuring yourselves and the public that you have taken every reasonable precaution. As a profession, we cannot take for granted that normal practices and procedures are sufficient while there is such heightened criticism. Correctly or incorrectly, allegations as to the professional competence and even honesty of election officials is in question by highly vocal groups. So read the recommendations contained in this Member Alert with the viewpoint that you may want to examine every facet of your ballot and voting equipment security. Many of the GAO recommendations are common sense or even common practice in many jurisdictions. And while we may disagree with the GAO on their acceptance of some of the criticisms as valid, there are some basic conclusions that will be good to examine. Heidi has done a good job here of distilling 102 pages down into something more readable. Read and then take time to start rethinking all of your own security practices and preparations.

## **GAO Report Continued: Electronic Voting Systems Security and Reliability Recommendations**

As a follow up to our last alert on the recent GAO report, "Elections: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed," we present the second and final e-mail discussing specific recommendations the GAO makes for the elections community and the EAC.

In the report the GAO identifies common practices that if implemented would address key security and reliability issues of electronic voting systems. Many of the GAO recommendations are similar to security standards and measures that are already in place, but encourage further research and documentation on the problems occurring at every stage of the election system process from product development to management. The GAO stresses at different points in their recommendations that vendors and election officials should review lessons learned from recent elections and implement relevant mitigation steps to address known security weaknesses. The report also encourages states to adopt the most current version of the national voluntary voting standards or guidelines.

Specific recommendations related to product development, as stated by the GAO, encourage developers to define security requirements and specifications for voting systems early in the design and development process. The GAO emphasizes that voting systems are unique in their security needs and require applicable laws, national standards, and other external influences and constraints that govern the development of systems.

Other recommendations suggest developers begin to include in systems: audit logs that record all activity involving access to and modifications of the system, including the time of the event, the type of event and its result, and the user identification associated with the event. The final recommendation of the GAO regarding system development warrants that systems employ adequate logical access controls over software and data files. This would require periodical change of passwords and would prohibit the use of vendor-supplied or generic passwords.

GAO recommendations relating to the election official's responsibilities are mainly concentrated in the acquisition and management phases of the voting system cycle. They encourage election officials to include security requirements, evaluation and test procedures in their Request for Proposals with the intent to prevent security and reliability problems from the beginning. In terms of management practices, the GAO suggests that election officials plan for poll worker training early in the process and ensure that all training classes and materials include information on the security of voting systems and on election security procedures.

Additional GAO recommendations in the management phase of the election cycle, suggest that election officials include employees with expertise on their administration teams. The teams should conduct risk analysis of voting systems in order to identify possible vulnerabilities. In order to ensure that all components on the voting system meet required standards and have been properly tested the GAO report recommends that election officials require that vendors submit tested and certified versions of the voting system to NIST's Library. GAO recommends election officials create procedures for handling election day equipment failure, including contingency plans: if voting machines malfunction during voting, they do not have to be repaired or removed from the polling place on election day, but can be examined at a later time to determine the root of the problem.

The GAO recommendations specific to election operations concentrate on the position state and local authorities should take on securing their systems before during and after an election. These recommendations suggest that sensitive activities in the election process, such as vote tabulation and the transporting of ballots or election results be performed by more than one person or observed by representatives of both major parties. Procedures for a chain of custody for all sensitive equipment (such as memory cards, ballots, and voting machines) should be identified and should thus be protected against unauthorized access before, during, and after an election. A post election audit of voting systems should be conducted to reconcile vote totals and ballot counts, even if there is no recount scheduled. An audit of the election system and process should be conducted after Election Day to verify that the election was conducted correctly and to uncover any possible security breaches.

In terms of recommendations for testing voting systems the GAO recommends that during the development phase developers should verify and validate the security controls on the system before deployment in order to ensure that the controls are working properly and effectively and that they meet the operational security needs of the purchasing jurisdiction. States and local governments should require that voting systems be certified against federal standards and then continue to conduct logic and accuracy testing on voting machines before the election to ensure that they accurately record votes.

The main recommendations of the GAO center on the role of the EAC. The GAO lists specific actions for the EAC, in combined efforts with NIST and the TGDC, to tackle. These recommendations include defining specific tasks, outcomes, milestones, and resource needs required to improve the voting system standards. The GAO also recommends that the EAC establish policies, criteria, and procedures for certifying voting systems that will provide direction until the national laboratory accreditation program is in place. As a resource of information for the election community, the GAO suggests the EAC with NIST establish a process for continuously updating the National Software Reference Library to effectively identify and circulate information to assist state and local governments in their efforts to ensure the security and reliability of specific voting systems. Other EAC efforts recommended by the GAO promote the development of a process for sharing information, with election officials, in a timely manner on the problems and vulnerabilities of voting systems. This process would also share recommended practices related to security and reliability.

Per the GAO, the complexity of assuring the accuracy, integrity, confidentiality, and availability of voting systems will continue to be a challenge with new technologies and developments, but with the combined efforts and proper concern of the election community, the security and reliability of electronic voting systems will continue to ensure fair and smooth elections.