



REP. HENRY A. WAXMAN
RANKING MINORITY MEMBER
COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES
OCTOBER 2005

Fact Sheet

GAO Finds Need for Continued Federal Efforts to Improve Electronic Voting Systems

Overall Findings

In October 2005, the Government Accountability Office released a comprehensive analysis of the concerns raised by the increasing use of electronic voting machines.¹ Overall, GAO found that “significant concerns about the security and reliability of electronic voting systems” have been raised (p. 22). GAO indicated that “some of these concerns have been realized and have caused problems with recent elections, resulting in the loss and miscount of votes” (p. 23).

According to GAO, “election officials, computer security experts, citizen advocacy groups, and others have raised significant concerns about the security and reliability of electronic voting systems, citing instances of weak security controls, system design flaws, inadequate system version control, inadequate security testing, incorrect system configuration, poor security management, and vague or incomplete standards, among other issues. ... The security and reliability concerns raised in recent reports merit the focused attention of federal, state, and local authorities responsible for election administration” (p. 22-23).

Specific Problems Identified by GAO

Based on reports from election experts, GAO compiled numerous examples of problems with electronic voting systems. These included:

Flaws in System Security Controls

Examples of problems reported by GAO include (1) computer systems that fail to encrypt data files containing cast votes, allowing them to be viewed or modified without detection by internal auditing systems; (2) systems that could allow individuals to alter ballot definition files so that votes cast for one candidate are counted for another; and (3) weak controls that allowed the alteration of

¹ GAO, *Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, But Key Activities Need to Be Completed*, at 3 (GAO-05-956) (Sept. 2005)

GAO FINDS NEED FOR CONTINUED FEDERAL EFFORTS TO IMPROVE ELECTRONIC VOTING SYSTEMS

memory cards used in optical scan machines, potentially impacting election results. GAO concluded that “these weaknesses could damage the integrity of ballots, votes, and voting system software by allowing unauthorized modifications (p. 25).

Flaws in Access Controls

Examples of problems reported by GAO include (1) the failure to password-protect files and functions; (2) the use of easily guessed passwords or identical passwords for numerous systems built by the same manufacturer; and (3) the failure to secure memory cards used to secure voting systems, potentially allowing individuals to vote multiple times, change vote totals, or produce false election reports. According to GAO, “in the event of lax supervision, the ... flaws could allow unauthorized personnel to disrupt operations or modify data and programs that are crucial to the accuracy and integrity of the voting process” (p. 26).

Flaws in Physical Hardware Controls

In addition to identifying flaws in software and access controls, GAO identified basic problems with the physical hardware of electronic voting machines. Example of problems reported by GAO included locks that could be easily picked or were all controlled by the same keys, and unprotected switches used to turn machines on and off that could easily be used to disrupt the voting process (p. 27).

Weak Security Management Practices by Voting Machine Vendors

Experts contacted by GAO reported a number of concerns about the practices of voting machine vendors, including the failure to conduct background checks on programmers and system developers, the lack of internal security protocols during software development, and the failure to establish clear chain of custody procedures for handling and transporting software (p. 29).

Actual Examples of Voting System Failure

GAO found multiple examples of actual operational failures in real elections. These examples include the following incidents:

- In California, a county presented voters with an incorrect electronic ballot, meaning they could not vote in certain races (p. 29);
- In Pennsylvania, a county made a ballot error on an electronic voting system that resulted in the county’s undervote percentage reaching 80% in some precincts (p. 29-30).
- In North Carolina, electronic voting machines continued to accept votes after their memories were full, causing over 4,000 votes to be lost (p. 31).

GAO FINDS NEED FOR CONTINUED FEDERAL EFFORTS TO IMPROVE ELECTRONIC VOTING SYSTEMS

- In Florida, a county reported that touch screens took up to an hour to activate and had to be activated sequentially, resulting in long delays (p. 31).

Current Federal Standards and Initiatives Are Ineffective and Are Unlikely to Provide Solutions in a Timely Fashion

GAO reported that voluntary standards for electronic voting, adopted in 2002 by the Federal Election Commission, have been criticized for containing vague and incomplete security provisions, inadequate provisions for commercial products and networks, and inadequate documentation requirements (pp. 32-33). GAO further reported that “security experts and some election officials have expressed concern that tests currently performed by independent testing authorities and state and local election officials do not adequately assess electronic voting system security and reliability,” and that “these concerns are amplified by what some perceive as a lack of transparency in the testing process” (p. 34).

The GAO report indicated that national initiatives to improve voting system security and reliability of electronic voting systems (such as updated standards from the Election Assistance Commission; federal accreditation of independent testing laboratories; and certification of voting systems to national standards) are underway, but “a majority of these efforts either lack specific plans for implementation in time to affect the 2006 general election or are not expected to be completed until after the 2006 election” (p. 43). As a result, GAO found that “it is unclear when these initiatives will be available to assist state and local election officials” (p. 43). According to GAO, “Until these efforts are completed, there is a risk that many state and local jurisdictions will rely on voting systems that were not developed, acquired, tested, operated, or managed in accordance with rigorous security and reliability standards — potentially affecting the reliability of future elections and voter confidence in the accuracy of the vote count” (p. 53).

Recommendations

GAO made several recommendations, primarily aimed at the federal Election Assistance Commission (p. 53). GAO recommended that the EAC should:

- Collaborate with appropriate technical experts to define specific tasks, outcomes, milestones, and resource needs required to improve voting system standards;
- Expeditiously establish documented policies, criteria, and procedures for certifying voting systems; and
- Improve support for state and local officials via improved information dissemination information on voting machine software, the problems and vulnerabilities of voting machines, and the “best practices” used by state and local officials to ensure the security of electronic voting machines.