July 18, 2006

The Honorable Vernon Ehlers
Chairman
Committee on House Administration
1309 LHOB
Washington DC 20515

Dear Chairman Ehlers:

As Chair of the U.S. Public Policy Committee for the Association for Computing Machinery (USACM), I commend Congress for reviewing issues related to voting machines, testing practices and standards. Ensuring that voting is accurate, error-free, secure and accessible to all registered voters is of great importance. However, as experts in computing, we have grave reservations about the safeguards in place with many of the computerized voting technologies being used. New federal standards and a certification process hold promise for addressing some of these problems, but more must be done ensure the integrity of our elections. We recommend that Congress and the Election Assistance Commission (EAC):

- Create a formal feedback process that will ensure that lessons learned from independent testing and Election Day incidents are translated into best practices and future standards.
- Make the testing process more transparent by making the testing scope, methodologies and results available to the public.
- Ensure that the guidance for usability and security standards provides performance-based requirements and is clear so as to minimize the variance of human interface designs from jurisdiction to jurisdiction.
- Create a mechanism for interim updates to the standards to reflect emerging threats, such as newly discovered security defects or attacks.
- Require voter verified paper trails and audits to mitigate the risk associated with software and hardware flaws.

Testing, Certification and Reporting

Thirty-nine states require federal certification of their voting systems, which is currently handled by independent testing authorities (ITA). They test the systems against the 2002 Voting System Standards (VSS). Ideally this testing would discover any flaws

in the system and allow for corrections before subsequent elections. However, in May 2006, a new report[1] was issued outlining several security vulnerabilities in one brand of certified electronic voting machines. Many computer scientists were stunned by the fundamental nature of these defects, and noted that the reported defects were the most egregious security vulnerabilities known to date. This was not, however, the first time serious security vulnerabilities were revealed.[2,3,4]

There are several gaps in our testing and certification system that need to be addressed even if we have more robust standards for voting systems. First, there is no corrective mechanism to ensure that flaws found during testing are fixed before subsequent elections. Second, the guidelines are being construed quite narrowly; if a flaw is found that is not explicitly prohibited by the guidelines, a system is still certified. It is unclear how such flaws can be successfully addressed under the current certification process. Finally, there is a clear need to create a formal system for reporting problems in the field and improving the standards based on these reports. This step will allow election officials throughout the country to be informed of potential problems and that experiences can inform the federal standards.

Under the Help America Vote Act (HAVA) the EAC is responsible for certifying voting systems through accredited laboratories. The National Institute of Standards and Technology (NIST) is taking over the accreditation process of ITAs from the National Association of State Election Officials. Federal involvement may make the testing and certification process more independent, but not necessarily more transparent.

Currently, voting machine vendors are the clients of the ITAs. Typically, they are the only recipients of the testing results, which are considered to be proprietary. This is not unusual. Certification testing of other products that the public relies on, such as aviation software and medical devices, is also proprietary. A key difference is that if an aviation system fails, the failure is reported to the FAA and investigated. If a medical device fails, the FDA investigates. Where the investigation demonstrates flaws in the management, manufacture, design, or testing of the aviation system or medical device, these flaws become public record and the operating rules and or equipment standards are adjusted accordingly. Investigation reports are public records.

Our country is far from having any such formal system for voting. We should have a system to ensure that lessons learned from multiple jurisdictions are feedback to vendors, states and federal officials, and then incorporated into standards and best practices. Often the real-world conditions of an election reveal errors that have not been detected by testing. The only organized incident reporting system for voting

---

[1] Harri Hursti, May 11, 2004, "Diebold TSx Evalution Black Box Voting," Black Box Voting, http://www.blackboxvoting.org/BBVtsxstudy.pdf

[2] Tadayoshi Ohno, Adam Stubblefield, Aviel Rubin, Dan Wallach, May 2004, "Analysis of an Electronic Voting System, IEEE Symposium on Security and Privacy 2004." *IEEE Computer Society Press*, http://avirubin.com/vote.pdf

[3] RABA Technologies LLC, January 20, 2004. "Trusted Agent Report Diebold AccuVote-TS Voting System," http://www.raba.com/press/TA_Report_AccuVote.pdf

[4] David Wagner, David Jefferson. Matt Bishop, February 14, 2006, "Security Analysis of the Diebold AccuBasic Interpreter," California Voting Systems Technology Assessment Advisory Board, http://www.ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf

equipment that has been employed recently is a limited, all-volunteer project sponsored by several non-profit groups.

Further, Congress should seek to make the certification process and testing results more transparent, and, like incident reporting, have a formalized system for incorporating the results into federal standards. The public should know the results of voting system tests and the certification tests of ITAs. California and New York State are taking steps to make their processes more transparent. Federal incentives also could strengthen the independence and transparency of the testing process. Incident reporting and transparent testing results would make it much more likely that vendors and elections officials would implement the lessons learned both from their own practices and from other jurisdictions.

Voting Guidelines

The new 2005 Voluntary Voting System Guidelines (VVSG) improve on the 2002 VSS, but they are not sufficient for ensuring that electronic voting systems are secure, reliable, usable and verifiable. It is unclear whether the level of guidance in the 2005 VVSG is adequate to guarantee that all eligible voters will be able to understand and use the new voting systems. In the area of human factors, the 2005 standards still leave too much to the discretion of local jurisdictions and are based on functional requirements instead of performance-based requirements. This is also a general problem with the security standards. While the EAC recognizes the problem, it is not in a position to act quickly.

The guidelines process is far from timely. The 2005 VVSG will take effect in December 2007 – two years after the standards were approved. In that timeframe it is difficult to refine the guidelines to handle problems not already covered. NIST is helping develop the next VVSG, but that will likely not be implemented before elections in 2010. Viruses and other security attacks operate in minutes and days, not months or years. A new method of developing and implementing interim guidelines quickly is necessary to respond to new problems.

Paper Trails and Audits

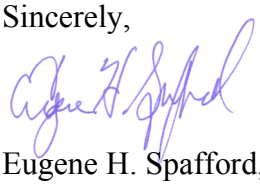
Even with improved standards and a process more responsive to emerging threats, the best designed and tested systems will continue to have flaws. We've seen numerous examples of security threats in software for commercial systems and critical infrastructures. Flaws, unfortunately, are inherent in any complex software system. There are formal mathematical proofs that testing is incapable of finding all accidental software flaws, and finding purposely concealed flaws is even more difficult. It is also possible to have unanticipated hardware or operational failures as well as accidents that can corrupt or lose vote totals held in memory of some voting machines.

To mitigate these risks we recommend paper trails and audits. Voting systems should enable each voter to inspect a physical record to verify that his or her vote has been accurately cast, and to serve as an independent check on the result produced and

stored by the system. Making those records permanent – not based solely in computer memory – allows for an accurate recount. We are encouraged by the actions of 36 states that have either established voter verified paper trails as law or purchased equipment capable of providing voter verified paper trails.

Thank you for taking the time to consider this important issue. Ensuring that computer based systems are secure, reliable, usable, and ultimately trustworthy will require ongoing involvement of technical experts, usability professionals, voting rights advocates, and dedicated election officials in the U.S. and other countries. We stand ready to provide technical guidance to Congress on this and other issues. Please contact ACM's Office of Public Policy should you have any questions at (202) 659-9712.

Sincerely,



Eugene H. Spafford, Ph.D.
Chair
US Public Policy Committee of the Association for Computing Machinery

cc: Members of the Committee on House Administration and House Committee on Science

About ACM and USACM

With over 80,000 members worldwide, The Association for Computing Machinery is an educational and scientific society focused on advancing computing as a science and a profession. USACM serves as the focal point for ACM's interaction with U.S. government organizations, the computing community, and the U.S. public in all matters of U.S. public policy related to information technology.