



Massachusetts Institute of Technology
Engineering Systems Division

Working Paper Series
Executive Summary

ESD-WP-2007-04

PATHWAYS TO A TRUSTED ELECTRONIC VOTING SYSTEM

Final Report – ESD.10

Jeremiah Connolly
Romain Lévy
Johnathan Lindsey
Judith Maro
Juan Martin

Massachusetts Institute of Technology
Technology and Policy Program

January 2007

EXECUTIVE SUMMARY

In 2002, Congress passed the Help America Vote Act (HAVA) [1], largely in response to voting irregularities in the 2000 presidential election in Florida. Congress intended that HAVA resolve the lingering public confidence issues arising from inconsistent local election administration procedures, punch card voting machines, and voter registration. With HAVA, Congress authorized payments to the states to implement significant reforms of the voting system. However, the use of electronic voting machines to meet HAVA requirements threatens to damage public confidence in the voting system.

Several reports have been published that note security flaws in voting systems in use all over the country [2]. California sued a manufacturer claiming that the company had misrepresented the security of its voting machines and falsified certification information [3]. In Ohio, a battleground state, recount irregularities also resulted in a lawsuit [4]. The public outcry and enormous media attention on these problems prompted Congress's Government Accountability Office (GAO) to launch an investigation [5].

SCOPE

The right to vote provides the foundation for a democratic government. A lack of public confidence in voting systems results in *de facto* disenfranchisement and a government elected by a subset of the population. The advent of electronic voting has tested public trust because it requires a greater leap of faith that a vote is being cast accurately, privately, and securely. Consequently, the central question that this report addresses is:

Which combination of technology and policy options will be most effective in increasing voter trust in electronic voting?

There have been many research reports [6-8] that recommend improvements to electronic voting processes. However, few have framed the question from the voter's perspective; that is, what actions initiated by federal, state, and local policymakers will make the most difference to the individual voter?

We approached our central question by examining four areas that influence public trust in electronic voting. They cover the following aspects: technical security, system testing and certification, conflicts of interest and local stakeholder participation.

Technical Security

As Direct Recording Electronic (DRE) machines continue to grow in their use across the country, computer security experts and many advocacy groups have raised significant questions about the technical security of the machines. Numerous studies [2, 9-12], each with differing methodologies, are consistent in their findings that current technical security standards for these machines are particularly inadequate in hardware, data, and access security. These security problems are not novel; other entities, such as the banking industry, have created secure and trusted systems for their customers. Although it is impossible to create a voting system that is absolutely secure, technical security improvements are needed to improved public trust in electronic voting.

Recommendation 1. The Election Assistance Commission (EAC) should improve technical security for DRE machines by:

- (1) strengthening protection of the machine's removable memory,
- (2) using stronger passwords for voter and supervisor access,
- (3) using stronger encryption mechanisms for voter and election data, and
- (4) removing electronic voting machines from communications networks.

System Testing and Certification

Certification of electronic voting machines is presently carried out by three Independent Testing Authorities (ITAs) who perform only functional testing of machines in accordance with EAC guidelines. The lack of robust penetration testing to challenge system security has led to significant machine flaws being missed by the ITAs [9, 10, 13-15]. Testing is paid for exclusively by vendors; therefore, the circumstances create a monetary dependency that calls into question the neutrality of the certification agencies [10, 14]. Additionally, the voting machine testing process is significantly more opaque than other government testing processes, and the lack of information available to the public seriously undermines confidence.

Recommendation 2a. The EAC should require penetration testing of electronic voting systems, and full test results should be released in a comprehensive, standardized report.

Recommendation 2b. Congress should establish an equipment testing fund that would be jointly supported by the federal government and the states to pay for testing and certification services.

Voting systems may also have two important emergent properties. First, security flaws which may be undetected at the scale of ITA testing may emerge when a system is used at full scale. Second, the user experience (and the trust which develops from that experience) may

be very different in the laboratory and open-system settings. Pilot testing of new systems will aid in the discovery of emergent problems before states are “locked in” to a technology choice. Congress recognized this potential and designated money for a pilot testing program in HAVA, but it has not yet funded the program.

Recommendation 3. Congress should follow through with its pilot testing commitment in HAVA by funding the EAC to pilot test and demonstrate novel voting systems.

Conflicts of Interest

Public concerns regarding the security of electronic voting systems are not only technical, but also result from perceived political and financial conflicts of interest among state and local election officials. In 2000, Secretary of State Katherine Harris served as an honorary chairman of the Bush campaign while presiding over the 2000 Florida recounts. The same situation occurred in 2004 in Ohio.

State and local election officials currently do not have uniform requirements to report and eliminate financial conflicts of interest. Corporate corruption already significantly endangers public trust in elected officials, but the potential for collusion between voting machine vendors and election officials threatens the foundation of an independent, democratic government.

Recommendation 4. State and local election officials should voluntarily end partisan participation in political campaigns and through campaign contributions. State and local election officials should also immediately divest themselves of all direct financial holdings in any corporation that manufactures or tests voting machines.

Local Stakeholder Participation

The Supreme Court’s finding in *Bush v. Gore* and Congress’s passing of HAVA significantly shifted election administration responsibility to the states, when it historically had been the domain of local election officials. Yet, local expertise is more crucial in questions of electronic voting because of the variation in the capabilities of poll-workers and the local electorate to cope with these systems. States differ in the level of local stakeholder involvement in procurement, implementation, and education decision-making as well as the amount of control delegated to local election officials [16].

The experiences of many states in their HAVA implementation suggest that increasing representation of local election officials in any decision-making entities can be expected to increase public support [17, 18]. Successful voter education efforts by local jurisdictions have increased the transparency of the process and allowed local election officials to build relationships that have engendered public trust.

Recommendation 5. States should choose to involve local election board officials and the general public in their procurement, implementation, and education decision-making.

CONCLUSION

This report provides a set of comprehensive recommendations designed to build public trust in electronic voting. We cover topics related to technical security, system testing and certification, conflicts of interest, and local stakeholder participation. The recommendations are directed to federal and state policymakers concerned with increasing voter trust in electronic voting systems. We expect that implementing these recommendations will have a positive effect on the public's perception of the voting process, and we urge that action be taken before the 2008 election.