Massachusetts Institute of Technology
Engineering Systems Division

Working Paper Series

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

Pathways to a Trusted Electronic Voting System

December 2006

Committee Members

Jeremiah Connolly
Romain Lévy
Johnathan Lindsey
Judith Maro
Juan Martin

(intentionally blank)

TABLE OF CONTENTS

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.

1.0 INTRODUCTION

In October 2002, the Help America Vote Act (HAVA) was passed by Congress and signed into law by President Bush. Partly as a response to voting irregularities that occurred in the 2000 presidential elections, the legislation was drafted to improve the administration of elections nationwide. In order to accomplish its intended goal, HAVA created the Election Assistance Commission (EAC), provided funding for states to replace outdated voting systems, and created minimum standards for states to adhere to in federal election administration [1]. Via HAVA, Congress directed the EAC to issue voluntary guidelines to help interpret its mandatory requirements and to oversee the certification/decertification of voting systems [1]. In order to receive federal HAVA funds, states were required to replace lever and punch card voting systems by the January 2006 deadline [1]. Consequently, most states have implemented electronic voting systems.

Although Congress intended HAVA to increase public confidence in the electoral system and to decrease the possibility of fraud, the introduction of electronic voting systems has done the opposite. Constant hacking of computers and networks, devastating viruses, and ubiquitous security updates have caused many Americans to worry about the safety of their votes. Government and university-funded studies have uncovered significant security flaws in systems currently deployed across the country [2, 5, 15]. In precincts where the voting process is entirely electronic, election officials and voter advocates question if electronic audits would be able to detect inconsistencies in voting records without paper ballots for review.

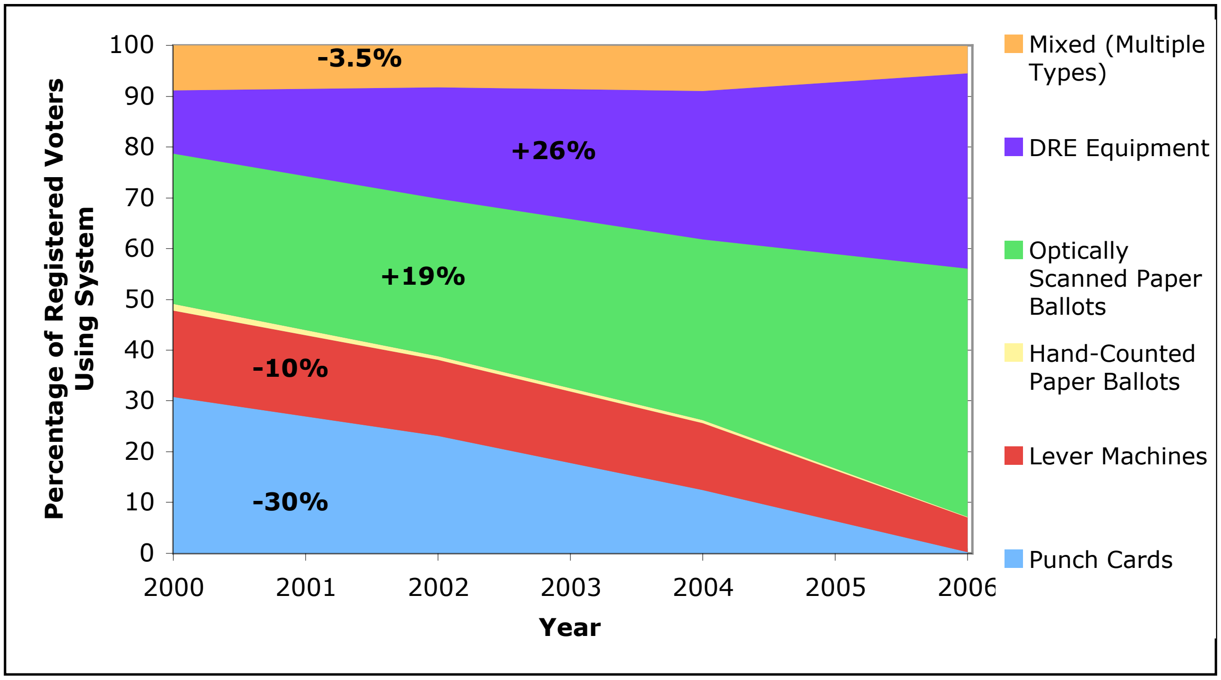
The public outcry and enormous media attention on these problems prompted the Government Accountability Office (GAO) to launch an investigation. While the GAO concluded that the EAC was taking the appropriate steps to secure the voting system, it predicted that those necessary changes would not be in place for the 2006 election cycle [5].

For more detail on the US electoral process in general or the development of HAVA specifically, refer to Appendices A and B.

1.1 MOTIVATION

In November 2006, 170 million people registered to vote [19]. Of those, approximately 150 million voters (87.3 percent) used electronic voting equipment, and 55 million of those who used electronic systems cast their ballot using entirely new equipment. Since the November 2000 elections, the use of electronic voting equipment has increased from 41.9 percent to almost 90 percent. Figure 1 shows that the debate to use electronic voting systems rather than paper or mechanical systems is over – many states have already committed themselves to using these systems. As shown, the use of DRE machines has grown by 26% from 2000 to 2006, while optical scan machines have grown by 19%. As the right to vote and participate in elections is the cornerstone for any democratic government, it is imperative that public confidence in electronic voting systems is protected and actively maintained.

Figure 1. Percentage of Registered Voters Using Various Election Systems[19]



1.2 SCOPE

Creating a voting system that is fast, secure, and easy to use is essential to encourage widespread participation and representation. In a time when voter opinion of the election process seems especially low, researchers and policy makers alike are working to find solutions that will increase voter participation. The task of creating a working voting system is much too large for one report; therefore, it is important that we define the scope of the report by clarifying the central question and contribution, limiting our focus to a specific electronic voting system, and outlining the roles of involved stakeholders.

1.2.1 Central Question and Contribution

Developing a voting system introduces tradeoffs among equity, efficiency, and system security. In this discussion, we define an efficient voting system as one that collects and counts votes with minimal labor and funding requirements. We also define a secure and equitable system as one that accurately collects and tabulates exactly one vote per citizen while maintaining the voter's anonymity. Although it would be ideal to obtain a system that is highly efficient, highly equitable, and highly secure, it is not possible to optimize all three.

We therefore look for methods that will achieve an optimal balance between efficiency, equity, and security. Consequently, the central question that this report will address is:

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

Because the question focuses on how to increase public trust, this report will provide recommendations from the voter's perspective. From this angle, the report will explore ways in which the current voting system framework can become both secure and trusted. Our focus on trust leads us to explore and analyze intangible factors not included in the multitude of published technical studies. Unlike other studies, this report aspires to create recommendations that will improve both the reality of voting system security and the perception of it. Our recommendations are directed to federal and state policymakers concerned with increasing voter trust in electronic voting systems.

1.2.2 Defining Electronic Voting

Electronic voting systems are systems in which a person's vote is stored in a database and tabulated using a software program. With the enactment of HAVA, the adoption of electronic voting machines has accelerated since 2002 – today only 1 percent of all votes cast and counted use paper ballots.

Electronic voting systems are part of a much broader and complex system, the electoral process, which they support by increasing efficiency and reducing errors that existed with older mechanical technologies. Among other things, state and local election officials hoped to clarify voter intent (*e.g.*, avoid over-voting and under-voting), increase usability for the disabled and language minorities, and resist fraud in future elections.

There are two types of electronic voting systems: Optical Scan machines and Direct Recording Electronic (DRE) machines. Optical scan machines are based on technology similar to that used in scoring standardized tests or lottery tickets. In precincts with this system, people vote by filling in a ballot. Once the voter has made his selections, he submits the ballot to an election official where it is scanned and tabulated using optical-mark-recognition equipment. In 2004, 35.6 percent of all registered voters used optical scan ballots; this year, 48.9 percent of all registered voters were projected to use optical scan ballots [19]. DREs, on the other hand, allow voters to make their choices on a computer. In most cases, voters register their preferences through a touch screen and submit their preferences electronically. Among many advantages, DREs are able to detect voter errors such as under-voting and over-voting as well as provide local customization and greater accessibility for people with disabilities.

For the purpose of this report, we will use the term *electronic voting systems* to refer only to those that employ DREs. DRE machines have grown in usage from 12.9 percent in 2000 to almost 39 percent in 2006 [19]. With its increasing presence in the nation's electoral system, many computer security experts, election officials, and voter advocates have expressed growing concern about DRE machines [2, 9, 10]. They worry that significant shortcomings in software/hardware security and reliability may cause a crisis during a national election. Others, like the Verified Voting Foundation, worry that the absence of paper records may make it difficult for officials to detect possible fraud. Unlike DREs, optical scan machines have largely avoided criticism, in part because the technology for these systems has matured and paper records (scan ballots) would be available for audit if they were to fail.

We focus on DREs because they are the fastest growing voting technology, their deficiencies have been highly-publicized, and they represent a greater disruption to voter trust than optical scan machines.

1.2.3 Identifying Stakeholders

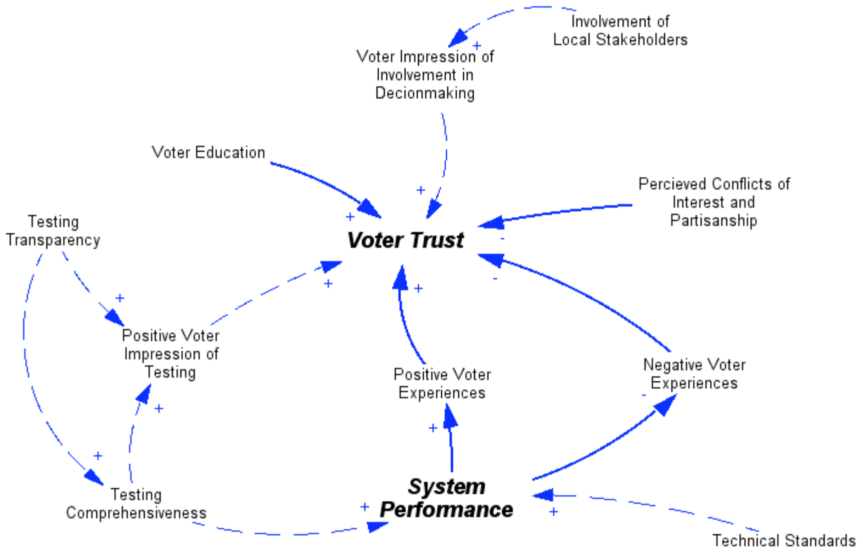
Relevant stakeholders in this problem include the federal and state governments, state and local election officials, independent testing agencies (ITAs), machine vendors, and voters. In the electoral process, federal and state governments both set standards that govern elections. The federal government sets mandates for the conduct of federal elections. In some cases, it may provide funding incentives for the states to update their voting systems in accordance with federal directives. State governments have oversight responsibilities for election administration and also enact state-specific election law. To some extent, local election officials may be involved in the development of voting system standards, but their involvement is usually limited to the implementation of federal and state policies. ITAs are agencies that use federal standards (as published by the EAC) to certify which voting machines are appropriate for use in federal elections. The EAC decides which testing agencies have the authority to certify machines; currently three organizations are allowed to certify and decertify machines. Some states have additional certification boards that test voting systems for compliance with state-specific regulations. Machine vendors are the agents that produce and sell voting machines. Four vendors comprise the majority of the market: Diebold, Sequoia, Hart InterCivic, and Election Systems & Software (ES&S) [19]. Other less involved stakeholders include political parties, candidates, and potential entrants to electronic voting machine market.

1.3 METHODOLOGY

We have broken down the central question of this report into four research areas that address specific problems concerning public trust in electronic voting: technical security, system testing and certification, conflicts of interest, and local stakeholder participation. In each section, we further investigate a specific problem using background information, scientific reports, case studies, and news articles. For each focus area, we make a recommendation and include a discussion that details relevant implementation challenges. We conclude with a final plan of action.

Figure 2 represents our conceptual model of how the aforementioned four concepts relate to system security and voter trust. In the causal diagram, arrows marked "+" indicate positive relationships, while arrows marked "-" indicate negative relationships. Strong and weak relationships are designated by solid and dashed lines, respectively. For example, more positive voter experiences contribute to voter trust, while more negative voter experiences detract from voter trust. Throughout the report we refer to this model, using it to show how our policies are expected to improve system security and voter trust.

Figure 2. Causal Diagram of Model Relating Policies to System Security and Voter Trust


Involvement of Local Stakeholders
Voter Impression of Involvement in Decionmaking
Voter Education
Percieved Conflicts of Interest and Partisanship
Testing Transparency
Voter Trust
Positive Voter Impression of Testing
Positive Voter Experiences
Negative Voter Experiences
Testing Comprehensiveness
System Performance
Technical Standards

1.4 ISSUES NOT ADDRESSED IN THIS REPORT

As stated earlier, "electronic voting systems" is a topic too large to be studied and discussed comprehensively in one report. To make the task of identifying key components of a trusted voting system easier to handle, several important issues will not be addressed in this report, either because they have already been studied extensively or not studied enough. In this report, voter registration systems, electronic voting systems with open source code, and voter verified paper record (VVPR) legislation will not be addressed.

1.4.1 Voter Registration Systems

The voter registration system is an integral subcomponent of our society's electoral process. By authenticating which individuals are allowed to vote in certain locations, the voter registration system defines communities. Prior to HAVA's enactment, each county in a state had the authority to manage their own registration systems. However, in section 303 of HAVA, the federal government mandated that each state use a "single, uniform, centralized, computerized statewide voter registration list" [1]. Although the new voter registration systems share some of the same security and efficiency issues as electronic voting, a full consideration of registration system policies includes other important issues such as privacy. Several research organizations, such as the National Research Council, plan to study voter registration systems in depth.

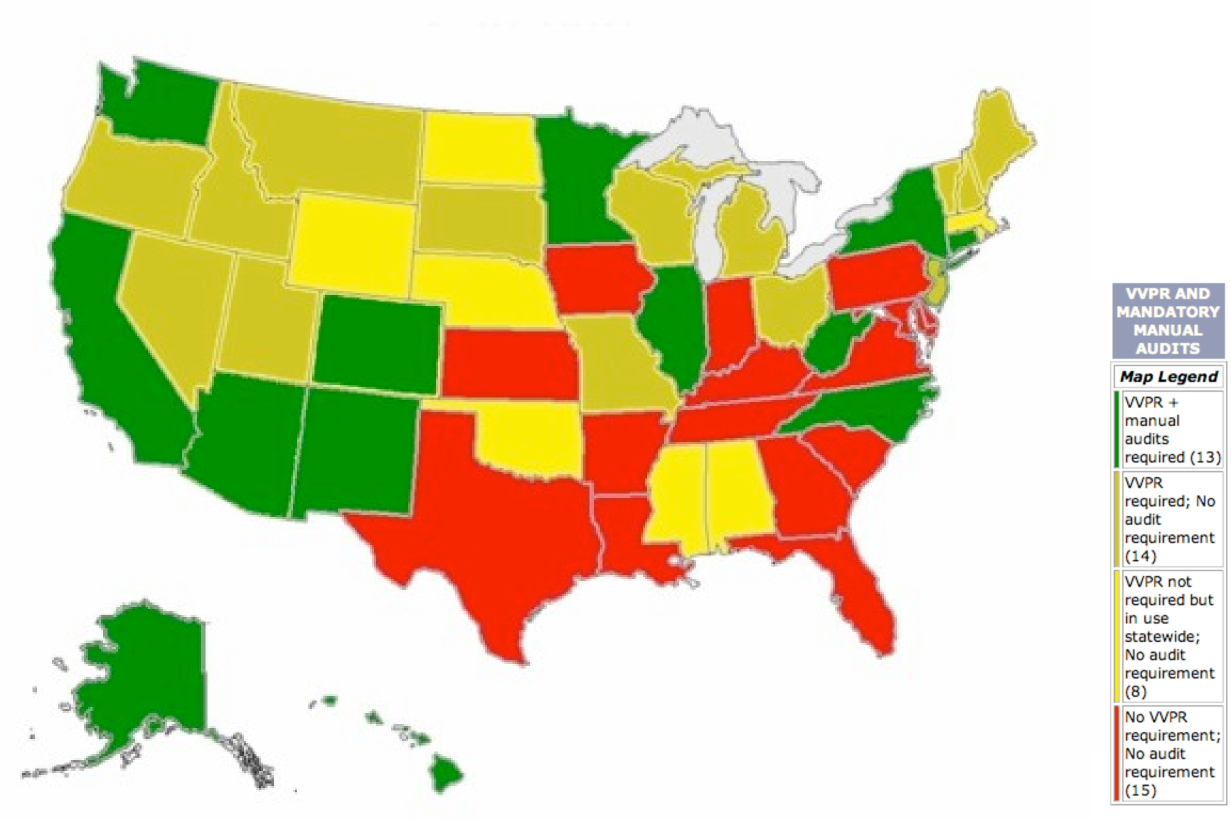
1.4.2 Voting Systems Using Open Source Code

Many computer security professionals advocate the use of open source software in voting systems [20]. In these systems, the core of the software used in electronic voting machines would be "open to the general public for use and/or modification from its original design free of charge" [21]. Advocates argue that open source systems are more appropriate for elections because they reinforce the spirit of open elections and improve the quality of the code, as more people are able to evaluate it [20]. However, several studies have shown that open source code is no more reliable or secure than proprietary code [20]. A recent MIT study has also shown that most open source code is viewed and modified by only a few people [22]. There have been several attempts to create open source systems for Internet voting, but no successful systems have emerged. Nevertheless, open source voting systems is an interesting research area that requires several in-depth studies before any judgment or recommendation can be made.

1.4.3 Voter Verified Paper Ballots

At the end of the voting process, voters expect to confirm that their intentions were reflected by their ballot. Most of the initial voting technologies that used paper ballots allowed the user to easily validate his or her vote. As DRE machines become more prevalent in the electoral system, voters must trust that what the system displays on the touch screen prior to confirmation will be recorded correctly. For some states, simply trusting that an electronic voting system will work correctly is not enough. As displayed in Figure 3, 27 states require VVPR for elections employing electronic voting system [23]. Another 8 states use VVPR statewide without legal mandates. It is clear from the states' overwhelming adoption of VVPR that paper records are a necessary component to a trusted and secure voting system. With this trend of support for the extra measure, VVPR appears to be a matured policy. Therefore, VVPR will not be discussed in the report although we support its inclusion in future federal standards as a mechanism for increasing voter trust.

Figure 3. State Voter-Verified Paper Record Legislation or Regulation[23]


VVPR AND MANDATORY MANUAL AUDITS
Map Legend
VVPR + manual audits required (13)
VVPR required; No audit requirement (14)
VVPR not required but in use statewide; No audit requirement (8)
No VVPR requirement; No audit requirement (15)

2.0 TECHNICAL SECURITY

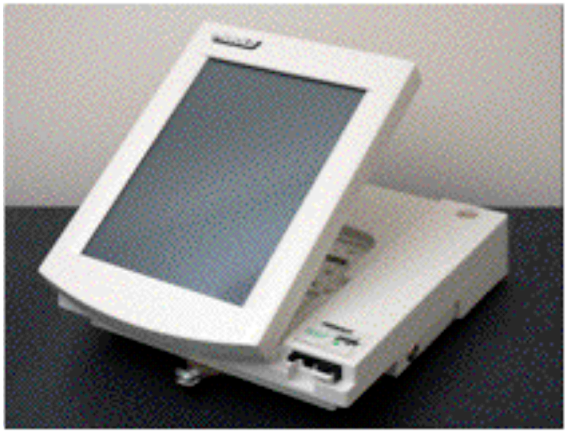
User trust in any system is the product of demonstrated security and reliability; people naturally trust what they know will work by experience. The discussion of how to increase voter trust in electronic voting systems must therefore begin with an evaluation of current DRE machines. In the following section, we begin by exploring how DREs work and how they interact with other important actors in the electoral process. We then continue by presenting evidence from a variety of scientific studies to show that the security of DREs currently implemented across the country is inadequate. More specifically, these studies will show that there are significant code, platform, and physical vulnerabilities that must be mitigated in order to avoid significant problems in the 2008 election. We believe that strengthening passwords, encryption mechanisms, and physical protection of the machines will substantially increase electronic voting security in both future and currently deployed machines.

2.1 BACKGROUND INFORMATION

2.1.1 Normal Operation of DRE Machines

From the voter's perspective, DRE machines work by digitizing the entire ballot-casting process. Normal machine operation begins when a registered voter is given a smart card with a password at the precinct. He then inserts the smart card into a reader and enters his password. The machine uses this information to confirm the voter's identity and then displays the ballot on a touch screen. The voter indicates support for candidates or ballot initiatives by pressing those options on the touch screen. At the end of this process, the DRE machine displays a summary of the person's votes. In order for his vote to be recorded and available for tabulation, the voter must confirm that this summary is correct; he accomplishes this task by pressing a confirmation button. The person's vote is then stored on a removable memory card. At this point, the ballot-casting process is complete and the DRE machine returns the smart card to voter [24]. Figure 4 displays Diebold's AccuVote TS machine. For a brief explanation of the components commonly found on DRE motherboards, refer to Appendix C.

Figure 4. Diebold AccuVote TS Machine [25]



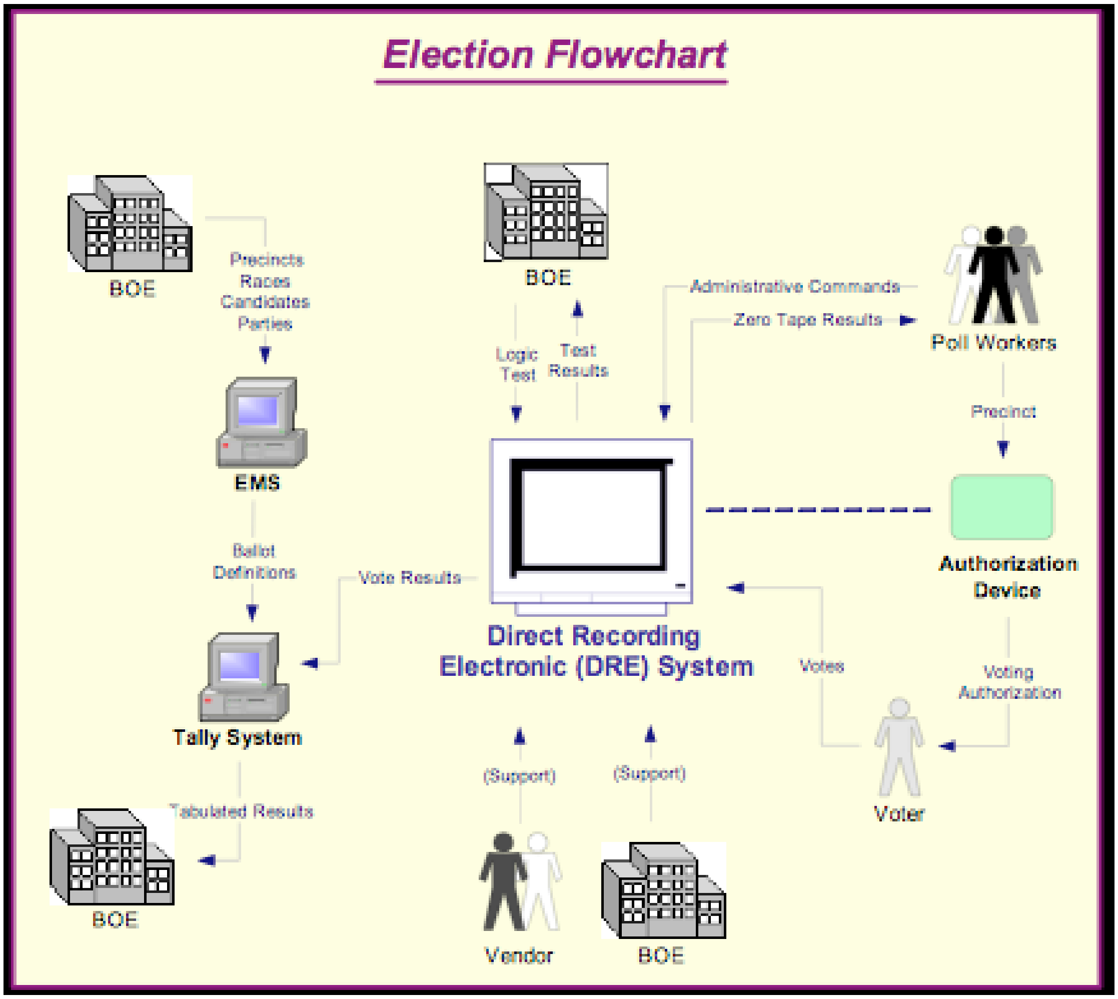
2.1.2 DREs in the Electoral Process

Figure 5 is a system diagram that describes how DRE machines operate in a general election by displaying the various interactions between a state's Board of Elections, poll workers, voters, and vendors [11].

In this diagram, the Board of Elections (BOE) is responsible for installing Election Management Software (software that creates ballot definitions for the DREs) on a computer at their headquarters. Workers at the BOE also perform logic and accuracy testing and verify the results prior to an actual election. If they observe a problem, they will attempt to troubleshoot the machine or contact vendors for additional assistance. In the event the vendor has to repair the machine, the machine is still required to successfully complete logic and accuracy testing before being deployed.

The poll workers set up the booths, open the DRE for voting, and authorize voters to vote during an actual election. During the election, voters must be authorized to vote and to use the machines. While voting, the DRE prevents the voter from over-voting and under-voting. The machine presents the ballot choices for review prior to confirming the ballot. Before the polls open, poll workers print a zero tape from the DRE to ensure there are no pre-existing votes recorded on the unit; afterwards, poll workers print results from the DRE machines and post one cumulative result for the precinct. The results are recorded on one media device (memory) and sent to the BOE for certification. Finally, the poll workers shut down the DRE machines and store them in a secure location.

Figure 5. Flowchart of Election Implementation Using DRE Systems [11]



As the BOE receives the media devices from the precincts, they are placed in a media reader where the Election Management Software tallies the results. Finally, the BOE certifies and releases the results after all precincts reported their results.

2.2 SPECIFIC CONCERNS AND VULNERABILITIES

2.2.1 Code Risks

Several studies, including the CompuWare 2003 Technical Assessment [11], have identified two specific code risks that were common across DRE machines. First, many machines lack effective encryption measures to protect data. In several cases, manufacturers employed hard-coded encryption methods that were easy to break or no encryption at all. Encryption is important because it works to protect information (ballot definitions, voter data, results) from being intercepted and reviewed by unauthorized agents [24].

Second, current electronic voting software and hardware do not have any mechanism to authenticate software installed on the ROM [25]. Authentication mechanisms work to prevent the system from unknowingly executing malicious code from on-board memory. In studies conducted at Princeton and Johns Hopkins Universities, surveyors found that some machines (particularly, the Diebold AccuVote machines) ran code installed on the ROM without checking whether or not it should be executed. Edward Felten of Princeton University, in a study analyzing Diebold's AccuVote TS vulnerability to attacks, demonstrated that it was relatively easy to install and run code attacks from the system memory. Once on the system, the code could execute two kinds of attacks: Vote-Stealing Attacks or Denial-of-Service Attacks [25].

Vote-stealing Attacks

A Vote-Stealing Attack is one that takes votes from one candidate and gives them to another. In order to remain undetected, the attack would not change the total number of votes tallied. In his study, Felten observed that the DRE machine maintained two records of each vote (one in internal flash memory and one on removable memory card). The study demonstrated a successful vote-stealing attack could easily modify both records to make them consistent with the fraudulent results [25].

Denial-of-Service Attacks

A Denial-of-Service (DoS) Attack aims to make voting machines unavailable to voters and officials during an election. Because many precincts across the country have been gerrymandered to favor one political party over another, DoS attacks have become a serious concern. In Felten's study, the surveyors found it relatively easy to install malicious code that would run at certain times of the day (perhaps late in the day when polls are about to close) and cause the system to crash. As a result, system memory, software, and all records would be wiped out, causing an entire precinct to be disenfranchised. Furthermore, restoring a machine to its normal state is difficult; a service technician would be required to reinstall the software and reboot the machine from ROM. If a DoS attack were implemented on a wide scale across several precincts or an entire state, it is possible that the election system would break down [25].

Although this experiment involved only one model from one manufacturer, it does give a clear indication of how vulnerable these machines can be to outside attacks. By either of these methods, malicious code installed by an attacker could steal votes or break machines without being detected by election officials.

2.2.2 Platform Risks

One major platform risk identified by academics and computer security experts is the security of DRE smart cards. Several studies have shown that it is possible to duplicate supervisor or voter access cards. Although the risk of "home-brewed" access cards is considered a platform risk, it is a result of ineffective or non-existent encryption measures [2]. Surveyors in the CompuWare Technical Assessment tried to create fraudulent access cards but they found it very difficult to accomplish. Nevertheless, they still concluded that, if a person were able to create fraudulent access cards, it would have a high impact in the election process [11]. A later study conducted at Johns Hopkins University went further in the analysis of smart card security. In this study, the authors were able to demonstrate methods in which a smart card can be duplicated with or without knowing the protocol used between the voting terminal and legitimate smart cards [2]. Using Diebold's AccuVote TS machine as a test case, they determined that, if an attacker knew the communication protocol, mass production of fraudulent smart cards could easily be done using commercially available smart card readers and user-programmable smart cards. The study also presented three different methods that an attacker could use to learn the protocol. The easiest of the three methods involved using a wire-tapping device to record communication between the voting terminal and the smart card. In either case, if a hacker were successful in obtaining the necessary communication protocol, he could create fraudulent smart cards that would allow him to deploy a Denial-of-Service attack by prematurely terminating elections on the voting machine [2].

Another common platform risk shared by all electronic voting machine manufacturers is weak password protection for supervisor functions. Surveyors for the CompuWare study identified machines that used hard-coded passwords or passwords that were easily guessable [11]. Worse even, some manufacturers used a common password for all its machines sold nationwide. Diebold, in particular, used "1111" as its supervisor access pass-code for all its AccuVote TS machines sold throughout the country; it took the surveyors less than two minutes to guess the code [11]. With weak passwords to guard supervisor access, an attacker could close elections early or erase results. A third platform risk common in the machines examined in the CompuWare study is their ability to be connected to a network. Specifically, some machines use a daisy-chain configuration to connect multiple machines together; in examining the Hart InterCivic machine, surveyors found that if a connection to one machine were to fail, the entire network would fail [11].

2.2.3 Physical Risks

A primary physical risk identified by many computer security experts examining electronic voting machines has been the security of the memory cards. The memory cards used in electronic voting machines are the same ones used in personal computers. Studies have shown that it is possible to unlock or break the seals and gain access to the memory cards. A person with this access could damage the memory card or switch it with a fraudulent one; in either case, an attacker could render the machine useless [24].

Results from CompuWare's 2003 Technical Assessment can be found in Appendix D.

2.3 RECOMMENDATION

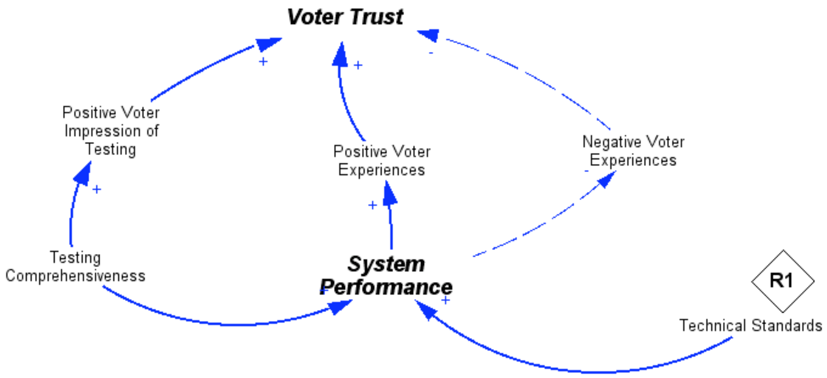
From the discussion above, it is clear that technical security of DREs must be addressed and improved prior to the next federal election in 2008. We present the following recommendations with the expectation that these improvements will significantly increase technical security in the upcoming election.

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.

We believe the above recommendations to improve the technical security of voting machines will directly increase voter trust. This relationship is displayed in Figure 6.

Figure 6. Recommendation 1 and the Model of Voter Trust


Voter Trust
+
+
-
Positive Voter Impression of Testing
+
Positive Voter Experiences
+
Negative Voter Experiences
-
Testing Comprehensiveness
System Performance
+
R1
Technical Standards

2.4 IMPLEMENTATION

Strengthening Protection of the Machine's Removable Memory

Better protection of the DRE's removable memory can be achieved in two ways. The first would involve utilizing stronger locking mechanisms on the outer latch covering the memory chips. As stated earlier, current locking mechanisms are commonly used in other applications and can be easily compromised. The second way that protection for removable memory can be improved is to create authentication measures for any code executing from the memory. By itself, the measure would not improve the physical protection of the memory, but it protects the integrity of the entire system from malicious code attacks. To provide maximum security, we recommend that the EAC require both these practices to be implemented in DREs.

Strengthening Encryption Mechanisms for Voter and Election Data

To strengthen protection of voter and election data, we believe the EAC should require the increased use of cryptography in voting systems. Stronger encryption measures should be added to the smart card authentication process to prevent the use of fraudulent cards in the voting system.

Using Stronger Passwords for Voter and Supervisor Access

Although Diebold's decision to make "1111" a standard password for supervisor access on all its AccuVote TS machines nationwide is an extreme case of poor password protection, the ease with which a password can be hacked does highlight the need for strong, robust passwords in critical systems. For most applications, we see that the number of permissible passwords increases exponentially as the number of characters increases. Precedent dictates that strong and robust passwords are long and complex, contain special characters, and are randomly generated (*e.g.*, no dictionary words). However, given that several layers of identity protection already exist in the voting process (specifically, voter registration and a "check-in" process at the precinct), passwords containing 6-8 alphanumeric characters are sufficient and easy for users to remember without writing them down.

Therefore, we recommend that the EAC require a minimum of 6-8 characters for passwords guarding supervisor and voter access.

Removing Electronic Voting Machines from Communications Networks

Removing electronic voting machines from any kind of communications network is the easiest method that can be used to improve DRE security. By isolating the machine, the possibility of remote attacks, interception of voter and election data, and interference from other machines would substantially be reduced [24].

In making this recommendation, we recognize that improving the current voting system must be done under certain political, cost, and time constraints. As many states have already fully implemented electronic voting systems, there is a significant cost in retrofitting thousands of machines with better software and hardware security mechanisms. To offset this cost, both federal and state governments would have to provide funding for local governments to secure their voting systems. Furthermore, the federal and state governments should require the electronic voting machine manufacturers to prove compliance of old and new machines with these new security requirements.

3.0 TESTING AND CERTIFICATION

The process of testing and certification of voting machines is central to the development of a trusted voting system. A strong testing system is one that will detect vulnerabilities, and communicate those vulnerabilities to users. In doing this, the testing system can be expected to exclude vulnerable voting systems while building public confidence in those systems that are suitably secure. The testing process also aids election officials in choosing a trustable voting system by informing their decision. Certification of voting systems can quickly communicate to users (both election officials and voters) that certain systems are suitably secure, but only if the testing behind certification is trusted.

The current testing and certification system in the United States is a wasted opportunity at best and a deeply flawed system at worst. We present evidence that testing has missed serious vulnerabilities in some electronic voting systems. Even if that were not the case, though, the current system misses opportunities to significantly increase voter trust in electronic voting systems. Testing is done by a small number of firms, results are kept confidential, tests are paid for by vendors, and tests are executed in unrealistic, small-scale scenarios. In order to increase the quality of testing and leverage the power of testing to improve voter confidence, we recommend that the EAC require penetration testing, adopt a more open reporting policy, and establish independent funding for ITAs.

3.1 CURRENT TESTING AND CERTIFICATION SYSTEM

Testing procedures are currently executed in a three-stage decentralized process. First, an ITA is responsible for federal-level certification by assessing whether the voting equipment meets the performance criteria outlined in a regulation known as the Voluntary System Standards (VSS) that later became the Voluntary Voting System Guidelines (VVSG). The second stage is state certification, which is completed by individual states and includes explicit tests for state regulatory requirements. If the state's voting standards are more stringent than national standards, a state test authority tests the state-required machine characteristics prior to proceeding to certification. Finally, acceptance is completed at the municipal level when voting equipment is delivered. Acceptance tests typically include a visual examination of the unit, an operational test of ballot casting and counting, and various accuracy tests.

Coincident with publication of the VSS standards in 1990, the National Voluntary Lab Accreditation Program of NIST was asked to assist the Federal Election Commission (FEC) in developing criteria to evaluate ITAs [26]. The intention was to then establish a formal accreditation program building on NIST guidelines, with NIST in the role of evaluating and accrediting ITAs [27]. However, NIST refused to commit to participation in either the guideline development or the actual lab accreditation without funding. The FEC's interim solution was to recommend that vendors submit their equipment to a major accounting/consulting firm or university "generally recognized across the country as competent in evaluating computer systems" [26]. The process was stalled for several years until the National Association of State Election Directors (NASED) voluntarily assumed responsibility for ITA certification in 1994 [28]. Unpaid members of the Voting Systems Committee on the NASED provided accreditation to testing laboratories with separate accreditations for software and hardware. The ITAs then tested voting equipment against the VSS; if the vendors were successful, their software or hardware was assigned an NASED qualification number. NASED also allowed for periodic re-accreditation and onsite inspections, although these were rarely conducted [28]. From 1994-2001, only one ITA, Wyle Labs, was granted accreditation, and 21 models of voting equipment were granted an NASED number [28].

The adoption of HAVA in 2002 proposed some modifications to the testing system. NIST is tasked with developing new guidelines for ITA testing that will supplement the VVSG by July 2008, and the current system will remain in place until then [1, 7]. This is therefore a unique window of opportunity to change the standards and organization of the testing process.

3.1.1 Evidence of System Testing Failure

There have been many publicized examples of significant voting system flaws passing ITA tests undetected. Some of these were chronicled by David Wagner in expert testimony to the U.S. House Committee on Science and the U.S. House Committee on House Administration [10], including the following:

- In 2004, over 4,000 votes were irretrievably lost in North Carolina by an ITA-certified system [29].

- In 2002, thousands of votes were mis-tabulated by vote-counting software in Florida. The error was noticed by an election worker and corrected for that election [30], however the same error happened again in two Florida counties in 2004 [31].

- In 2006, 100,000 “votes” (which were not actually cast by voters) were counted in Texas by and ITA-certified system [32].

In academic and independent security studies of ITA-certified voting machines (including some of the studies we explore in more detail in Chapter 2), numerous vulnerabilities and flaws have been exposed. These include:

- A Johns Hopkins University and Rice University review of ITA-certified source code that found “that this voting system is far below even the most minimal security standards applicable in other contexts” [2].

- Independent reviews commissioned by the State of Maryland that found “significant high risk vulnerabilities” in an ITA-certified machine [9, 12].

- Independent reviews commissioned by the Ohio Secretary of State that found the potential for high-impact but difficult to perpetrate attacks in four ITA-certified machines [11].

- A 2005 review that found that an ITA-certified optical scan system was highly vulnerable to a vote-stealing attack by someone with access to a memory card in the machine [33].

- A report by the State of California which found similar vulnerabilities to memory-card attacks in two ITA-certified machines [15].

- Testimony to Congress by the chairman of the Iowa Board of Examiners, Douglas Jones, that Wyle Labs (an ITA) had *assumed* in its testing of a certain machine that the encryption key the machine used was secure. Jones later learned that every machine manufactured by the vendor uses the *same* encryption key [34], which he compares to “the situation you would expect if all ATM cards issued by some bank had the same PIN…” [35].

Jones, as chairman of Iowa’s Board of Examiners, had access to some of the ITAs’ test results. He described the ITAs’ incomplete reports as…

> "…a black eye for the entire system of Voting System Standards promulgated by the Federal Election Commission and the National Association of State Election Directors. Not only did the I-Mark/Global/Diebold touch screen system pass all of the tests imposed by this standards process, but it passed them many times, and the source code auditors even gave it exceptionally high marks. Given this, should we trust the security of any of the other DRE voting systems on the market?" [35].

3.1.2 Root Causes of System Testing Failure

In the following sections we identify four features of the current system that contribute to its poor historical performance.

Weak Testing Standards or Execution

The current ITA system cannot guarantee that voting machines undergo rigorous testing prior to their deployment in elections. To give an idea of the strength of the system, an electronic voting system security expert testified to Congress that “in the history of the ITA system, no system ever failed qualification. Instead of a pass/fail system, the only options are 'pass' and 'hasn't passed yet,'"[14] and later, "the current process of qualification testing by ITAs is dysfunctional. Some of these systems contain security holes so severe that one wonders what the ITA was looking for during its testing"[14].

NIST reviewed a 2002 VSS update and found numerous discrepancies from its own security guidance for federal information systems [5]. Specifically, no voting equipment software is tested against NIST's Trusted Computer System Evaluation Criteria or the International Standards Organization Common Criteria [36]. NIST also criticized the testing procedures promulgated for their lack of penetration testing, *i.e.*, testing by specifically trying to attack the source code [5]. The functional testing that is required by the VSS simply tests that the system performs in the way that it was intended [36]. Functional testing is unlikely to ever trigger certain types of hidden code [36].

In cases such as those noted in the previous section, scientists have taken federally certified machines (those that have successfully completed testing by an ITA) and still discovered significant defects and vulnerabilities. These results suggest that either system standards are weak or the ITAs do not have the requisite skills to properly audit voting system software [13]. In either case a strengthening of the testing process is warranted.

Transparency

The opacity of the current testing scheme limits its usefulness in aiding decisionmakers while doing little to increase voter confidence in tested systems. Current rules define both ITA reports and state-commissioned independent reports as the property of the vendor [10]. As such, they are unavailable to the public and only available to state officials in some circumstances [10]. When states commission an independent test, they are often forced to sign non-disclosure agreements with the vendors. In the case of both the ITA and state-commissioned tests, the testing process is largely unknown. This situation hinders oversight and auditing measures to make the systems secure, and wastes an opportunity to communicate positive findings to the public and thus engender trust.

Conflicts of Interest

Under the current system voting machine vendors pay ITAs for their testing and national certification services. This situation creates a monetary dependency that may stress the neutrality of the certification agencies [14]. The potential for fraud exists, particularly in light of the fact that very few on-site inspections or reaccreditations of these laboratories has ever occurred [28]. Additionally, all versions of the VSS and the VVSG lack a prohibition of financial conflicts of interest, *e.g.*, whether a vendor is allowed to have stock in a testing laboratory [37]. Whether or not neutrality is compromised is less important in our analysis than the fact that compromises are possible, since perceptions of potential conflicts can be damaging to voter trust.

These potential conflicts have significant potential to undermine public confidence in the testing system. One scholar has recommended that the costs of testing laboratories be shared by the states on a pro-rata basis [14]. Another proposes that the EAC charge vendors a flat fee in order to be eligible for certification and use these funds to pay ITAs [10].

ITA Organization

As of 2003, only three ITAs were accredited and allowed to perform system testing [38]. Because the government requires ITA testing, the three ITAs operate as a *de facto* oligopoly. In this uncompetitive environment, the ITAs effectively set their own performance standards. Additionally, the small number of ITAs inherently makes any technical omission by these firms in the qualification process a potential catastrophe.

3.1.3 Recommendation

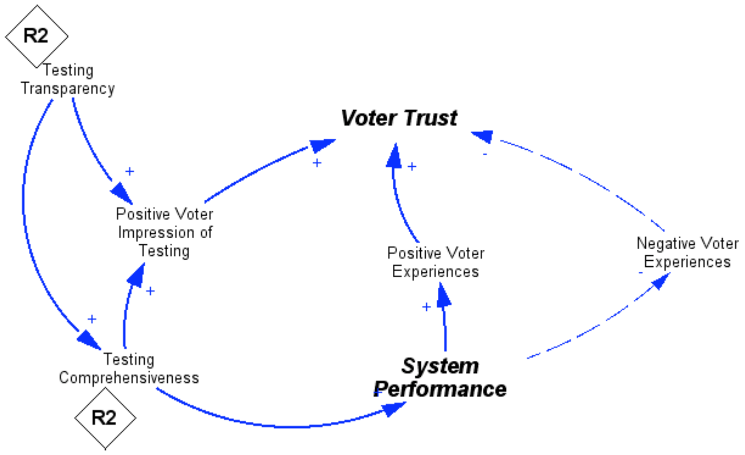
The current testing system relies on weak standards and lacks transparent reporting to stakeholders. ITAs operate in an uncompetitive environment and face potential conflicts of interest in their funding sources. In response to these issues we suggest the following reforms to the federal testing system:

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.

Figure 7 below shows this recommendation implemented in our model of voter confidence. Improving testing standards is an improvement of testing comprehensiveness and therefore should improve system performance. Additionally, improving testing transparency should both force testing agencies to be more comprehensive, improving system performance, and improve the voter impression of the testing process.

Figure 7. Recommendation 2 and the Model of Voter Trust


R2
Testing Transparency
Voter Trust
Positive Voter Impression of Testing
Positive Voter Experiences
Negative Voter Experiences
Testing Comprehensiveness
System Perfomance
R2
+
-

3.1.4 Implementation

Congress should establish annual funding to provide independent and comprehensive testing for new machines. This testing should be overseen by the EAC and NIST, but paid for from a general fund rather than by the vendors themselves. The funding scheme may be difficult to establish, but numerous proposals exist [10, 14]. Because we are proposing that testing standards be increased, we also feel it is important to test existing, already-certified machines. The government may have to bear the cost of recertification, but this one-time cost will greatly improve voter confidence in the installed system.

Testing results should be released to all stakeholders, including the general public, in the form of a standardized. This report should not reveal patentable information such as specific source code, but it should include enough information to communicate to the public how a system has performed in a comprehensive security test. The format of this report should be specified in the Procedural Manual for the Voting System and Testing Certification Program that is currently undergoing comment at the EAC.

The vendors are stakeholders with concentrated interests and significant political influence. Their opposition to this reform will be significant. Therefore, it will be important to communicate the importance of these reforms to state and local officials and voters in general. If these groups can be convinced to support the reforms, their alliance should overcome the political power of the vendors.

3.2 PILOT TESTING

Voting systems may have emergent properties in two important aspects. First, security flaws that may go undetected at the scale of ITA testing might 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.

Pilot testing goes beyond the "penetration testing" advocated in the previous section by testing machines in real, open systems at a relatively large scale. The best pilot tests also use standard experimental design, including control and experimental samples, in order to isolate the effects of the experimental technology.

Congress recognized the value of pilot testing by authorizing $10 million in HAVA for pilot testing in 2003, distributed by the EAC as grants with NIST aiding in the coordination and execution of these tests ([1], especially Section 281-283). This money was never apportioned in 2003 [39], though, and has not been mentioned in subsequent annual reports by the EAC [40, 41]. Pilot testing is also not mentioned in the 2005 VVSG [42].

In the following sections we present examples of pilot testing in the US and United Kingdom. Based on these examples, we recommend that Congress provide the funding for pilot testing it designated in HAVA.

3.2.1 Georgia's Testing Experience

Cathy Cox, Georgia's secretary of state, used problems encountered in Georgia and elsewhere during the 2000 election to catalyze a statewide election reform process [18]. Georgia took on this challenge without federal guidance. After the passage of HAVA, the reforms adopted by Cox's initiative were rolled into the state's HAVA plan. The state ran pilot tests of various technologies and solicited public comment in the technology choice through a variety of mechanisms including surveys and public meetings following the pilot tests [18]. The pilot tests gathered important information about voting systems, but the design of tests did not follow standard experimental design [17]. After a trial and public comment period, the state chose a single electronic voting technology to implement statewide, which it did by the 2002 elections. The reform was seen as successful by the public [43] (at least initially) and this success was partially attributable to the use of pilot testing [17].

3.2.2 United Kingdom Pilot Testing

While the UK has not experienced a voting crisis like the United States election of 2000, it is interested in improving the ease of use and security of its voting systems (an in depth look at the UK program, upon which this paragraph and the next are based, is presented in [17]). In 2001, the UK created the Election Commission (EC), which has used a "research-based model" [17] for developing, testing, and implementing new election systems. The EC's approach uses small-scale tests to measure how effective new systems are and what effects they have on voter satisfaction and confidence. These tests are "scientifically-based" [17], meaning that they include control groups and change one variable (*e.g.* the voting system) at a time. The tests attempt to quantify the results and isolate those changes that are due to the experimental change.

Pilot tests of various systems – including mail-in, Internet, touch screen electronic, mobile phone, and other systems – were executed in 2002, 2003, and 2004. Results of tests in previous years were used to inform and refine the design of later tests. A number of unforeseen issues emerged during the pilot tests. For example, issues with assuring vendor quality and ensuring adequate system support became more apparent as the scale of some piloted systems increased. An inadequately supported system may experience reliability problems or user errors, leading to improperly recorded votes and a poor voter experience. Pilot testing therefore identified an issue with significant implications for voter confidence in the new system.

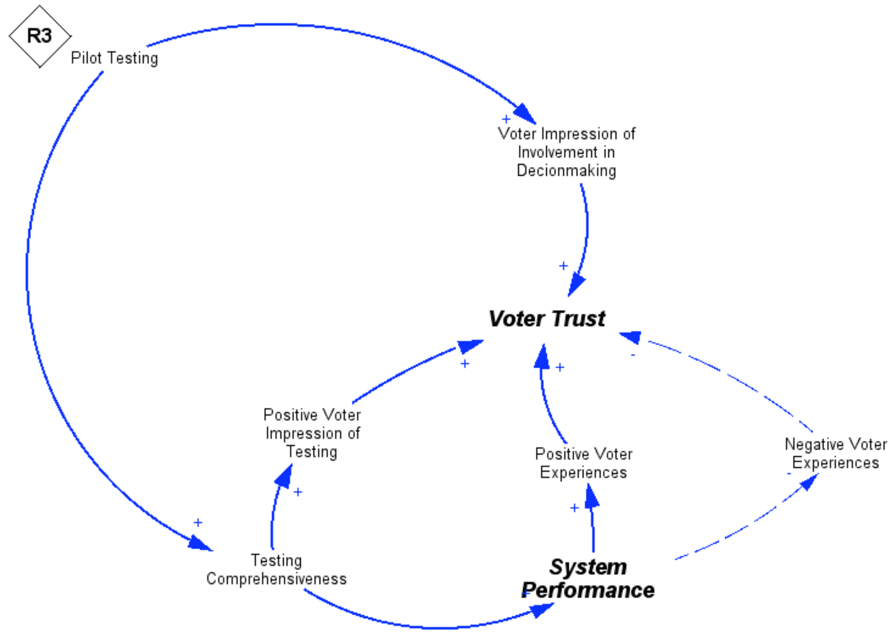
3.2.3 Recommendation

Pilot testing can be expected to detect emergent security flaws and user issues. Scientifically designed pilot tests have been used in the United Kingdom to successfully explore a variety of electronic voting options [17]. In Georgia, piloting helped inform system choice and, by demonstration, build voter confidence [17, 18]. While the GAO recommends pilot testing for government projects such as voting system development [44], in practice scientific pilot testing is not done in the US. We therefore recommend that Congress apportion the funding authorized by HAVA for pilot testing, and that pilot testing be included by EAC and NIST in any further changes to the Voting System Guidelines.

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.

Figure 8 shows this policy implemented in our model of voter trust. We expect pilot testing to improve testing comprehensiveness, and therefore both voter impression of testing and system performance itself. Additionally, the demonstration aspects of testing can be leveraged to improve voter impressions of their involvement in election system decisionmaking. Engaging voters in this way will develop trust.

Figure 8. Recommendation 3 and the Model of Voter Trust


R3
Pilot Testing
Voter Impression of Involvement in Decionmaking
Voter Trust
Positive Voter Impression of Testing
Positive Voter Experiences
Negative Voter Experiences
Testing Comprehensiveness
System Performance

3.2.4 Implementation

Congress should provide the annual funding of $10 million authorized by HAVA to pilot test voting systems in a variety of settings. States may be interested in using pilot tests to help them make decisions among systems, and vendors may be interested in using pilot testing to aid in product development and marketing. It may be possible to leverage both of these potential common interests in the form of federal-state and public-private partnerships, which may share the burden of testing costs.

As with Recommendation 2, vendors are likely to oppose this action as it makes them more vulnerable to exposure of flaws or trade secrets. However, pilot testing has already been included in the 2002 HAVA and simply funding the program should be enough to implement this recommendation.

4.0 CONFLICT OF INTEREST AND PARTISANSHIP

In exit polls following the 2006 federal elections**,** a significant number of voters said corruption and scandals in government were extremely important in their voting decisions [45]. Elected officials stand to gain politically and financially from influencing the procurement, testing, and certification of electronic voting machines. Voters should also be confident that both state and local election officials are free of partisan political influence. Therefore, in the following section we recommend a voluntary moratorium on partisan political participation of state and local election officials via campaign contributions, lobbying efforts, fundraising efforts, etc. Additionally, we also recommend that all state and local election officials immediately divest themselves of all direct financial holdings in any corporation that manufactures or tests voting machines. We believe that these near-term actions will send a strong message to the American people that the voting process is free of the influence of special interests.

4.1 PRECEDENT

Political neutrality of government officials is not a novel concept in the American tradition. Certain officials, like the Chairman of the Federal Reserve, are appointed for terms that span several political cycles. Theoretically, the length of the appointment is intended to insulate the official from politics. Similarly, federal judges are appointed to the bench for unending terms so as to avoid accountability to public opinion through the election cycle. In arguing for the life tenure of the judiciary, Alexander Hamilton stated, “That inflexible and uniform adherence to the rights of the Constitution, and of individuals, which we perceive to be indispensable in the courts of justice, can certainly not be expected from judges who hold their offices by a temporary commission” [46]. Additionally, the United States Code prohibits staff employees of the FEC and EAC from “tak[ing] an active part in political management or political campaigns” [47]. A staff employee of the FEC is also not allowed to receive or give a political contribution. Federally, policymakers have recognized the necessity of political neutrality as it relates to election administration.

There is also precedent for disclosing or eliminating financial conflicts of interest. Following the Watergate scandal, The Ethics in Government Act of 1978 was passed; it required financial disclosure statements from most federally-elected government officials and other members of the executive branch [48]. Additionally, the United States Code requires judges to disqualify themselves from proceedings in which the judge “has a financial interest in the subject matter in controversy or in a party to the proceeding, or any other interest that could be substantially affected by the outcome of the proceeding” [49]. We believe that state and local election officials should be held to the same standards as these members of the federal government.

It is important to note that in election administration, the perception of political and financial neutrality is just as vital as the reality of the circumstance. To extend the judicial metaphor, according to U.S. Code, "Any justice, judge, or magistrate judge of the United States shall disqualify himself in any proceeding in which his impartiality might reasonably be questioned" [49]. The use of the phrase "*might* reasonably be questioned" (emphasis added) implies that proof of impropriety is not required; instead, merely the perception of potential bias is enough to mandate recusal.

In the following chapter, we share anecdotes from Ohio, Maryland, and Nebraska in order to demonstrate how perceptions of the influence of competing interests damage confidence in electronic voting systems. We do not attempt to prove or disapprove any of the allegations of misconduct on the part of election officials; it is irrelevant to our analysis. Instead, we find that the perception of misconduct is more than adequate to stimulate voter distrust. This phenomenon is more significant in electronic voting systems than paper voting systems because of the increased lack of transparency in casting and counting votes. There is a greater leap of faith for the voter to make in casting an electronic vote than in filling out a paper ballot. Therefore, voter trust is more valued in electronic voting systems because it is harder to earn. Consequently, conflicts of interest are substantially more damaging.

4.2 EXAMPLES OF CONFLICTS

4.2.1 Ohio

In 2003, many state and local jurisdictions were getting ready to implement newly available HAVA funds in advance of the 2004 election. During the same time period, researchers at Johns Hopkins University published a detailed analysis of the security flaws of the Diebold AccuVote-TS DRE machine [2]. Therefore, it seemed surprising when Republican Secretary of State Kenneth J. Blackwell eliminated Sequoia Voting Systems as a potential bidder for Ohio's new HAVA-compliant system while allowing Diebold to place a bid. Because Diebold was a local manufacturer and supporter of the Republican Party, the move was viewed as a political favor that could be uniquely bestowed by the Secretary of State due to his power as the senior state election administration official.

It is notable that Diebold contributed $100,000 to the Republican National Committee during both the 2000 and 2002 election cycle [50]. Further, Diebold's chief executive Walden O'Dell invited one hundred top Republicans to his home for a fundraiser and famously stated “I am committed to helping Ohio deliver its electoral votes to the president next year” [51]. While the general public cannot demand non-partisanship from private vendors, the key point that must be understood is that voters saw Blackwell's decision to exclude Sequoia as a reward for Diebold's support of the Republican Party. Later, when a state judge issued a temporary restraining order that prevented Blackwell's action against Sequoia, it seemed to affirm the public's suspicion that Blackwell's motives were not purely in executing his public election administration duties [52].

To complicate the circumstances, the 2004 Ohio presidential election was marked by a high number of irregularities and forced recounts in many districts. Because of Ohio's importance to the presidential election, the controversy received national attention. Rep. John Conyers, the Ranking Member of the House Judiciary Committee, commissioned a special report on the problems. Two members of Congress invoked an 1887 statue that forced debate on the floor of both houses with respect to whether Ohio electors should be seated [53]. Vote-switching on electronic voting machines was one of the chief complaints among voters, resulting in more votes counted for a particular candidate than eligible voters in a precinct. Because Diebold had not maintained a neutral position politically and machine malfunctions like the vote-switching favored the Republican Party, the voters rightfully questioned the neutrality and fairness of the election.

Four lawyers filed a lawsuit to prevent the Ohio election from being permanently declared in favor of Bush-Cheney. Locally, the Ohio Supreme Court Chief Justice refused to recuse himself from that lawsuit even though the vote switching would have affected his own campaign for re-election that year [4]. A recount was conducted and certified by Blackwell despite the fact that he was also serving as co-chairmen of the Bush-Cheney campaign in Ohio. Surprisingly, Blackwell's conduct was legal because no conflict of interest laws prevented him from acting as chief elections officer and a head of a political campaign simultaneously. It is noteworthy that partisan conflicts of interest were not unique to the 2004 Ohio election. In 2000, Florida Secretary of State Katherine Harris was the honorary chairman of the Bush campaign in Florida while she simultaneously certified the Florida recounts [54]. In both cases, state law required recounts in order to certify the election results; and, in both cases, the Secretary of State had the final authority to direct recount procedures that ultimately decided the election. It is not only remarkable that these narratives are so similar, but that the American people have not demanded action on the part of state legislatures to prevent this situation from recurring.

In January 2005, Blackwell sent out a letter expressing gratitude to Republicans for helping deliver Ohio to Bush, stating "thankfully, you and I stopped [Kerry's election]" [55]. In that same letter, he requested contributions to his planned gubernatorial campaign for the following election cycle. Again, the impudence of Blackwell shocked the public. Rep. Conyers responded, "acknowledging the commingling of his official duty to ensure a fair election with his partisan duty to re-elect President Bush, evidences Secretary Blackwell's poor judgment at best, and the manipulation of election administration for partisan purposes, at worst" [55]. It is imperative that election officials maintain an heir of neutrality if they are to be trusted by the American public.

4.2.2 Maryland

In 2003, when the aforementioned Johns Hopkins researchers at the Information Security Institute first reported on the security weaknesses of Diebold DRE systems [2], Maryland was in the process of purchasing such systems for use in the 2004 presidential election. Following the Hopkins report, the state of Maryland hired Science Applications International

Corporation (SAIC) to study the problem. SAIC released their public report on September 2, 2003. It was 38 pages long and affirmed many of the security risks in the Diebold systems that had been reported earlier [9]. Despite the problems identified, Maryland purchased $55.6 million dollars worth of electronic voting equipment from Diebold [56].

The SAIC report was personally certified by Linda Lamone, administrator of Maryland's State Board of Elections and the president of NASED. As President of NASED, Lamone had a vested interest in demonstrating the robustness and accuracy of the ITAs because NASED was responsible for accrediting them. However, she also had a responsibility to the state of Maryland to aggressively pursue reports of security flaws in Diebold systems despite the fact that the ITAs had certified the machines. Lamone had an organizational conflict of interest because the many findings of the SAIC report posed the question of whether ITAs (and by association, NASED) were properly executing their duties during the testing and certification process.

In spite of the doubts raised in the report, Maryland officials expressed confidence that the problems could be solved prior to the 2004 primary election. Later, a 197 page unredacted, unedited version of the same report (containing the same SAIC tracking number) was leaked on the Internet [9]. Apparently, the ability to redact portions of the report was a condition that Diebold had secured during the contract in order to protect the use of proprietary information [9]. The 160 pages of information were allegedly removed prior to its submission to the State Board of Elections and the Governor of Maryland, and only Lamone had access to the full report. It was rumored that Lamone's competing interest in preserving the reputation of the NASED may have influenced her approval of Diebold's striking of information that was potentially vital to the decision-making process. With 55.6 million dollar state investments depending on the results, the omission of this data from the full report was not trivial. It is possible that if the full report were available to the State Board of Elections, they may have procured the electronic voting equipment in a different manner. Again, the perception of Lamone's conduct is the key point regardless of whether she actually acted in a disreputable way.

SAIC's impartiality, and by association, Lamone's, were also questioned when it was revealed that SAIC was a member of the Information Technology Association of America's Information Security Committee, an organization that works to improve public perceptions of electronic voting [57]. Shortly thereafter, the governor of Maryland found that a lobbyist for SAIC was also registered as a lobbyist for Diebold Election Systems and asked the state ethics commission to investigate [58]. While the state ethics commission later vindicated the lobbyist of any violations, the public perception of a conflict of interest for the consulting firm already existed. The credibility of SAIC's report was doubted, and therefore, it held no weight [59].

As a response, the Maryland state legislature hired a second firm, RABA technologies, to investigate the Diebold systems. The RABA study affirmed the security vulnerabilities of both the Hopkins report and the SAIC report [12, 60]. TrueVoteMD, an activist organization, then sued the state of Maryland to force the state to provide paper ballots for those that did not want to use the state-wide Diebold systems. During the lawsuit, Linda Lamone aggressively pushed the use of the Diebold systems, and testified to their security and accuracy [61]. Although TrueVoteMD was unsuccessful in their suit, the attention to Lamone's testimony caused the State Board of Elections to force her into paid administrative leave while they developed the paperwork to terminate her for cause [62]. The State Board believed that her ability to objectively administer elections was compromised. Lamone filed suit in Anne Arundel County Circuit Court to retain her job. A judge temporarily blocked the board's efforts and allowed Lamone to return to work [63]. Lamone remains in the job today despite open disagreement with the Governor and State Board of Elections. Public distrust of the chief state election official is damaging to the future conduct of all elections especially when public perception is that the official does not prioritize the interests of the voter first.

4.2.3 Nebraska

In some cases, the conflict of interest does not arise due to political affiliations or due to divided loyalties in the election process, but results from a financial interest that politicians, election officials, or other decision-making bodies may have in the commercial success of electronic voting machine manufacturers. In Nebraska, prior to Sen. Chuck Hagel's election in 1996, he was the CEO of American Information Systems, the predecessor of ES&S [64]. Following his election, Hagel retained some of his connection to the company via indirect means. Hagel disclosed to the Congress that $1.8M to $6.7M of his personal holdings were managed by the McCarthy Group which jointly owned ES&S with the Omaha World Herald [65]. ES&S machines counted ballots in all 93 of Nebraska's counties in 2002 when Hagel won re-election to his Senate seat [66]. With distrust of electronic voting systems already high, it is ill-advised for Hagel not to divest himself of his financial interest in ES&S. As a shareholder of ES&S, Hagel can theoretically influence the company’s behavior – a prospect that may distress voters. The vote-switching phenomenon that marred the 2004 election in Ohio or the inability of electronic voters to ensure that their vote was correctly counted further underscore the possibility (and temptation) of collusion between elected officials and voting machine manufacturers.

This problem is magnified and more concerning if the individual is a state or local election official. Because state laws vary tremendously with respect to the financial disclosure demanded of state and local election officials, it is difficult to track whether they have financial involvement in voting machine manufacturers or testing companies. While we were not able to find evidence that financial conflicts of interest among state and local election officials have previously occurred, it was disturbing that we were not able to find evidence that they could not occur. It is not uniformly illegal for state and local election officials that affect the procurement, testing, and certification of electronic voting machines to have direct financial interests in voting machine companies or testing companies. It is also not uniformly illegal for local election officials to engage in consulting roles with voting machine vendors.

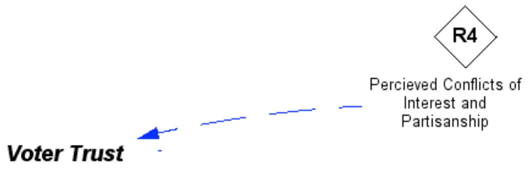
4.3 RECOMMENDATION

Because voter protection against conflict of interest concerns was not a part of HAVA in 2002,

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.

Figure 9 shows this recommendation implemented in our model of voter trust. Perceived conflicts of interest and partisanship have a direct negative impact on voter trust. By creating strategies to guard against these kinds of conflicts of interest, we believe that the electorate will have less reason to believe that their votes are not being counted accurately and securely.

Figure 9. Recommendation 4 and the Model of Voter Trust



4.4 IMPLEMENTATION

Although states control most aspects of the conduct of their election officials, all voters have a stake in ensuring that federal elections are conducted fairly and free of any potential bias. Several bills before Congress already include provisions to protect the voters against partisan and financial conflicts of interest. For example, the Count Every Vote Act of 2005 requires that chief state election officials, top-level executives, and owners of voting system manufacturers abstain from federal election campaign activities including contributions. The Voter Confidence and Increased Accessibility Act of 2005 requires standard-setting to ensure that testing laboratories do not "have a financial interest in the manufacture, sale, and distribution of voting system hardware and software, and is sufficiently independent from other persons with such an interest" [67]. While we would like to see these recommendations become federal law similar to the U.S. Code that prevents federal judges from participating in proceedings for which they have a conflict of interest, we acknowledge the long timeline associated with federal legislation and the potential legal challenges involved with demanding action from state and local election officials.

Legislative solutions require broad Congressional support. As many as nine different bills have been proposed in Congress that would amend HAVA in various ways. Most of them have not become part of the legislative agenda, and few of them have moved past committee consideration. However, we believe that a window of opportunity exists to consider these bills particularly in light of the anti-corruption theme of the 2006 federal elections and the promises of the 110th Congress. The electronic voting machine companies and testing companies would be ill-advised to publicly stand against conflict of interest provisions of any bill; however, these provisions are usually attached to bills that contain voter-verified paper trail requirements and other funding requirements that are more controversial and could be targeted in an attempt to bury the overall bill. Additionally, federal legislators may try to "soften" a ban on conflicts of interest by requiring simply a disclosure of political and financial activities instead. We firmly believe that voters will not be satisfied with simply a disclosure, but that voter confidence and trust is built by knowing that it is illegal for questionable political or financial affiliations to exist *per se*.

Another implementation challenge of federal legislation is the potential conflict with state election law. Because the state election officials in most states administer both federal and state elections, it is difficult to devise a federal policy on preventing conflicts of interest that is not potentially hostile to states' rights. Therefore, it is important that states also begin a legislative process to forbid conflicts of interest in parallel with the federal government. Many voting initiatives like VVPR requirements have been very successful as state-initiated actions[j1]. Additionally, it is more appropriate for state and local election officials to have their duties codified in the Constitution of each state.

With respect to the Linda Lamone case, it is important to recognize that the conflict of interest arose as a result of competing public duties. Because she served as the head of NASED, she had an interest in defending the testing process. However, she also had a competing interest as the head of the Maryland State Board of Elections in rigorously auditing that very testing process. There is an inherent conflict of interest whenever the auditor and the audited are the same entity. Legislatively, it would be difficult to pinpoint these particular circumstances because it is unusual that this condition exists. However, as Lamone found out when her colleagues and the governor began to publicly denounce her conduct, it is important to voluntarily disclose or remove these unique conflicts of interest. Moreover, HAVA demanded that accreditation of the testing laboratories be turned over from the NASED to NIST, so it is unlikely that this particular conflict will be a problem once new accreditation and testing guidelines are enacted.

Because of the difficulties in using legislative channels to achieve near-term goals, we are limiting our recommendation to administrative solutions. We perceive the voluntary moratorium as the best near-term solution to building voter trust. To increase accountability to the electorate, state and local election officials should sign statements that declare their freedom from any conflicts of interest, be they political, organizational, or financial. We also recommend that vendors themselves voluntarily refrain from political involvement although we do not believe they should have a legislated obligation to do so. In these cases, the filing of a company ethics policy as well as signing statements could demonstrate that vendors recognize the importance of conflict of interest to voters.

We do not believe that auditing or enforcement of these terms is unmanageable. Campaign contributions and partisan affiliations are well-tracked by public interest groups and the FEC. Also, there is precedent in the U.S. Code as to what constitutes political participation and undue financial conflicts of interest, and these rules could easily be applied to state and local election officials. Until federal or state legislation can be enacted, we believe a voluntary pledge via published signing statements is a simple solution that can greatly increase voter trust in electronic voting systems.

5.0 LOCAL STAKEHOLDER PARTICIPATION

The adoption of HAVA has shifted control of many election processes from precincts and counties to the states. In the following section we show that this shift has been widespread and includes some of the functions with the greatest public visibility, including voter education. Through case studies we show that increased local participation can be expected to improve voter perceptions of the voting system and the decisionmaking process that manages it. Based on this evidence, we recommend that states involve local stakeholders in their procurement, implementation, and voter education decisionmaking.

5.1 BACKGROUND

In 2000, the presidential election in Florida first exposed Americans to the widespread voting irregularities that occurred among local jurisdictions within one state. Not surprisingly, the variations were largely procedural, and involved the recount process, design and approval of the ballot, etc. Traditionally, control of these aspects of election administration has been the responsibility of local election boards because of their expertise in understanding the needs of the local electorate. For example, local election officials have potentially greater insight into the required number and the appropriate translation of Spanish ballots in their jurisdiction than state or federal entities. However, too much decentralization can lead to situations like the 2000 election in Florida in which "the standards for accepting or rejecting contested ballots might vary not only from county to county but indeed within a single county from one recount team to another" [68]. In *Bush v. Gore*, the Supreme Court held that states have a procedural responsibility to protect "one person, one vote" concepts such that each individual has an equally likely chance that their vote is counted accurately [68]. Legally, this landmark case formally codified the state-level burden in overseeing the proper conduct of elections, and recognized the significance of state-level decisions in election administration.

Similarly, when Congress passed HAVA, it significantly shifted responsibility for the conduct of election administration away from local municipalities in favor of statewide controls. Via HAVA, Congress set federal minimum requirements for voting systems and voting procedures [1]. Consequently, in establishing these requirements, Congress had to assign responsibility for implementation. It is interesting to note that Congress did not delegate implementation to local entities, who have historically held these responsibilities; it chose to delegate implementation to state entities via the HAVA State Implementation Plans. Decisions regarding voter education, election official training, poll worker training, voting system guidelines and processes were among the duties formally transferred from localities to the state [1].

5.1.1 Influence on Voter Trust

While we acknowledge that the centralization of authority may build voter trust by improving consistency and reliability in election administration, the shift of traditionally local decisionmaking authority to state officials has important implications for voter trust.. If desired, state policy makers can set voting system standards and procedures without any local input. This is a potentially disconcerting possibility when decisions are to be made about choosing and administering electronic voting systems. The success of electronic voting system implementation demands local knowledge as to the degree of technical awareness of the electorate, the technical savvy of volunteer poll workers, and the potential for breaches in the chain of custody of electronic voting machines. As was mentioned earlier in this report, electronic voting systems have been heavily criticized because of security vulnerabilities, equipment malfunctions, and inadequate poll-worker training. Local expertise can provide considerable insight into the ability of communities to overcome these obstacles. Local feedback can also contribute to developing preventative strategies that seek to build in procedural safety features that protect system security and voter confidentiality.

Figure 10. Purchasing Power for Voting Systems Based on HAVA Implementation Plans[16][1]

[1] Maps created using Map-Maker Utility available at http://monarch.tamu.edu

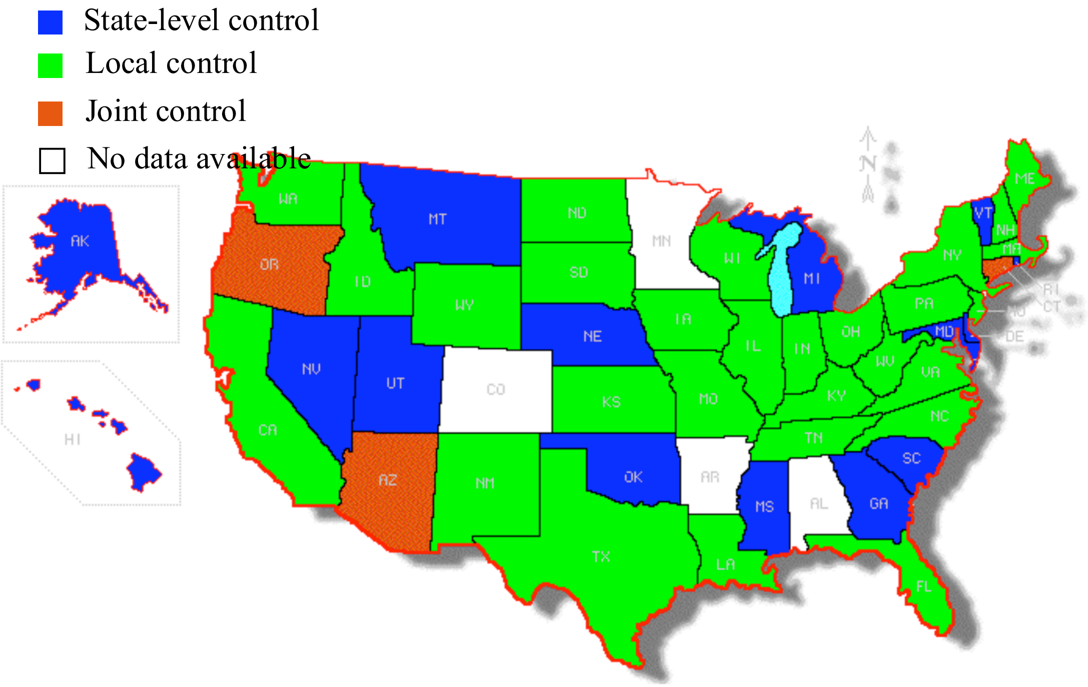


Figure 11. States Requiring a Uniform Voting Technology in HAVA Implementation Plans [16][2]

[2] Maps created using Map-Maker Utility available at http://monarch.tamu.edu

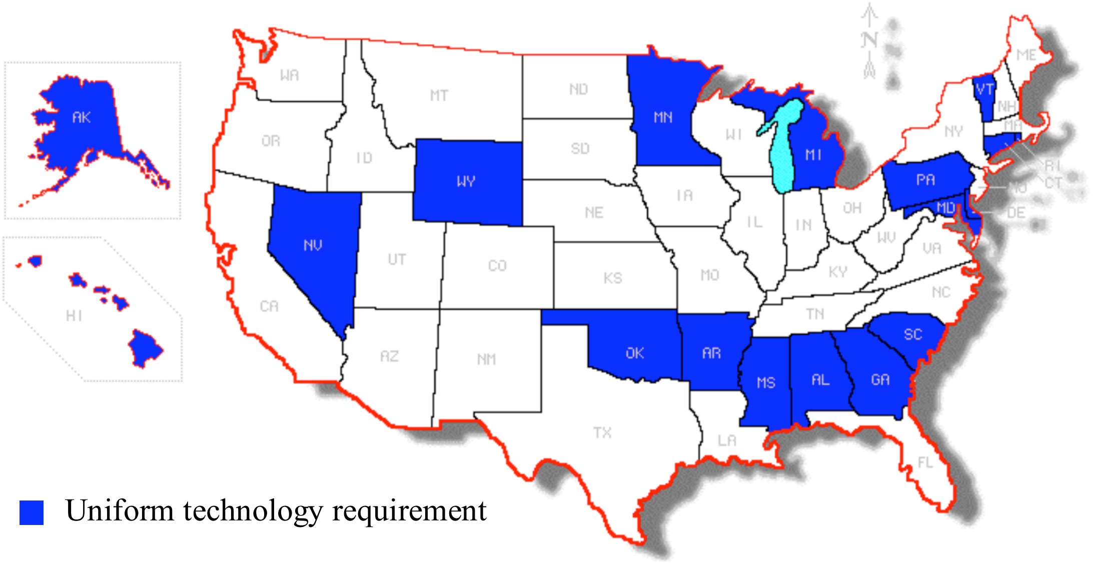
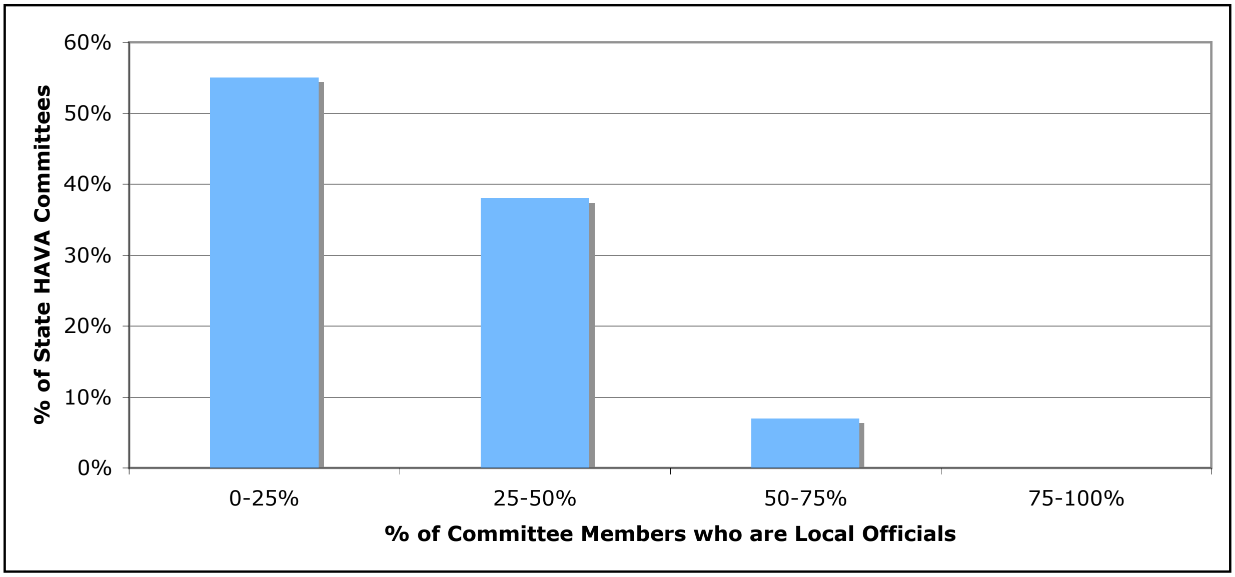


Figure 10 depicts the level on which procurement decisions regarding HAVA-complaint voting systems were made [16]. While approximately two-thirds of the states delegated purchasing machines to the local level, almost one-third maintained control at the state board of elections. Additionally, in their state HAVA plans, eighteen states have removed some of the decision-making process from local entities by mandating a uniform technology across all districts within the state [16]. Therefore, even if a locality is able to choose which voting machine they would like to purchase, they are limited to the state-mandated technology (*e.g.*, Alaska may mandate optical scanners). Figure 11 depicts states with a uniform technology requirement. In the most restrictive eleven states, state HAVA plans call for a uniform voting machine, removing all choice [16]. Additionally, only two states, Hawaii and Kansas, intended to delegate voter education initiatives to the local level [16]. The overall trend is one of historic shifts in responsibility from local to state levels.

If there is little or no local involvement in the HAVA-funded procurement, implementation, poll-worker training, and voter education processes, we find that state policy makers will also lose an opportunity to build voter trust. We recommend that states choose to involve local election board officials and the general public in their procurement, implementation, and education decision-making. By involving local stakeholders, electronic voting systems pose less of a challenge for voter confidence because voters will feel that they have participated in improving the voting process in their communities [69]. HAVA presented a convenient way to ensure local interests were represented because of the opportunities for local involvement in an individual state's HAVA planning committee. However, Congress gave states considerable discretion in choosing their planning committee members; specifically, it did not dictate the percentage of local planning officials on these committees. Again, a non-trivial minority of state planning committees had less than one-third of the committee reserved for local election officials, as shown in Figure 12. Additionally, transparent and open processes that solicit public comment prior to their implementation further increase trust. Only nine states made specific provisions for public involvement in the technology choice/procurement stage of their HAVA implementation [16].

Figure 12. Local Representation on State HAVA Planning Committees[18]



5.2 CASE STUDIES

In addition to the trends in implementation, the following three case studies provide insight into trends regarding local stakeholder involvement and the amount of control given to state and local levels. We explore the experiences of Georgia, California, and Florida in developing their HAVA implementation plans and use these cases to illustrate the variety of strategies (or lack thereof) to increase local involvement. Following that, we discuss the actions that are available to states now that many have already finished their HAVA implementation.

5.2.1 Georgia

In the 2000 federal election in Georgia, there was a residual voting rate (or undervote rate) of 3.5%, the second worst in the nation among reporting states [70]. Georgia Secretary of State Cathy Cox used this and other statistics as the centerpiece of her efforts to catalyze a statewide election reform process. Alvarez and Hall examined the Georgia case study to note the degree to which election administration procedures and reforms were influenced by local election officials and the general public [18].

On the surface, Georgia's HAVA implementation plan appears to be rigidly controlled by the state. Decisions regarding the choice of voting technology and the procurement process were centralized [16]. Cox even introduced legislation that required a uniform purchase of a single model of a particular technology for use in all of Georgia’s voting precincts. However, Cox moderated her seemingly hard-nosed stance on election reforms by encouraging local election officials to sit on the precursor to its HAVA implementation committee, called the

21st Century Voting Commission [18]. From a policy standpoint, we find Cox's strategy of local inclusion specifically compelling because local election officials were presumably insulted by the Secretary of State's report on the ineffective technologies and procedures in place in Georgia in 2000. By extending an olive branch to local stakeholders, Cox softened the admonishing effect of the report and mitigated the natural anxiety that usually accompanies revolutionary changes in the status quo. She appointed eight local election officials (her legislative maximum) to the eighteen-member Commission [18].

The Commission had a mandate to pilot-test and to select the uniform voting technology and machine to be used in the 2002 election. They held public meetings to educate voters on the process; performed exit polls to solicit public opinion during the pilot testing phase, and commissioned public surveys from the University of Georgia to gauge voter feeling on electronic voting. After the remarkably public trial and comment period, the Commission chose a single electronic voting technology (DREs) which it implemented by the 2002 elections, around the time of HAVA's enactment. Georgia's HAVA implementation committee included similar levels of local representation. Georgia was one of only three states whose HAVA committee was composed of more than 50% local election officials. Cathy Cox's strategy of local inclusion resulted in the political support necessary to enact sweeping reforms. In September 2001, only 56% of Georgians were very confident and 76% very or somewhat confident that their “vote was counted accurately,” but after the 2002 elections, those numbers had risen to 70% and 93%, respectively [43].

5.2.2 California

Alvarez and Hall [18] examined the case of California as a foil to Georgia. California also attempted to act quickly in response to problems with the 2000 election, but their progress was much slower. Alvarez and Hall described California’s policy process as pluralistic, where “political considerations [were] at the forefront of the policy process, with interest group pressures and the political interests of the principals determining the solution selected” [18]. Unlike Georgia, California's HAVA committee was composed of less than 15% local election officials. Instead, California included a wide variety of single-issue interest groups, including representatives of language minorities and the disabled, and advocates for and against paper auditing. While California's size and heterogeneous population probably necessitated the involvement of these groups to generate political support, the lack of local election officials gave the impression that the committee was forcing its implementation scheme on local jurisdictions without asking for their counsel. Additionally, the passage of HAVA and the promise of federal funding coincided with Secretary of State Kevin Shelley's election to office. He was known for his political ambitions and there was great distrust that he intended to use successful election reform in California for his own political gain [18].

In 2004, tensions between local election officials and the Secretary of State increased when Shelley decided to unilaterally de-certify electronic voting machines that were already chosen and in use by local jurisdictions. Shelley was responding to reports in the *Oakland Tribune* that Diebold had not certified the software elements of the encoders, bypassing the qualification and certification processes at both the state and national levels [71]. Internal

Diebold memos also contained discussion of Diebold's ability to trick the state and local testing process by only revealing certain parts of the system and concealing problems [71]. Consequently, Shelley withdrew his approval of the uncertified Diebold machines throughout the state. He considered allowing 10 of 14 California counties to use the machines in November, but only if Diebold resubmitted its system for certification as a new machine [72]. Additionally, he single-handedly enacted new requirements for VVPR for all DRE machines [72]. Shelley pursued this course of action without consulting with local election officials, and there was widespread suspicion that the decision was intended to advance his own political objectives.

Subsequently, Shelley was sued by individual counties who had purchased Diebold machines for his interference with their right to conduct municipal elections in the way they saw fit [71]. If the relationship between the Secretary of State's office and local election officials were not so strained, perhaps a dialogue would have been the preferred course of action as opposed to a lawsuit. The antagonism between the parties was one of many negative influences on voter trust. Of California voters in 2004, only 23% were very confident and 39% somewhat confident that the new electronic voting machines used in California would ensure that votes were counted accurately [73].

5.2.3 Florida

MacManus conducted a detailed case study of election reforms in Florida [74] (on which the facts in this section are based unless otherwise noted). In the wake of the 2000 elections, civil suits were filed against many local election officials, and some saw increased state control and uniformity as a way of avoiding lawsuits in the future. Election reforms passed in 2001 and 2002 by the state legislature outlawed certain voting technologies, but did not mandate specific technologies to replace them. Instead, decisions about voting systems were made at the local level. Florida's HAVA implementation also involved a moderate (25-30%) membership of local election officials [16]. Florida is not noteworthy for its local involvement in implementation planning, but it is unique in its focus on voter education strategies to involve public stakeholders and to build trust.

Florida devoted a significant amount of resources to increasing public participation in the election reform process through voter education initiatives. In the Election Reform Act of 2001, the county election supervisors were required to conduct voter education campaigns. Six million dollars were allocated for that purpose, and the voter education programs were crafted by the counties. By allowing local jurisdictions to address specific needs, the state acknowledged the importance of their expertise. The state undertook a supervisory role by evaluating the voter education programs for their cost-effectiveness. Additionally, the state seemed to be responding to the needs of the local constituents who, according to a statewide survey, demanded more voter education and better training for election officials and poll workers [75, 76]. Notably, Florida was the first state to recognize the importance of local voter education programs in building trust in election processes. It passed legislation requiring county election supervisors to provide voter education programs ahead of HAVA's passage. Funds were allocated for this purpose by the state, before Congress authorized any HAVA funds for this purpose.

In addition to executing major voter education initiatives for the 2002 elections, Florida deployed new voting technology (both electronic voting and optical scan machines) for the 2002 elections. In the elections of 2002, the turnout increased and the voter error rate declined substantially. While one cannot attribute all of these changes to education reforms, a new survey showed that the voters' confidence in the integrity of the process increased, as did the rating of the performance of local election officials by voters [75]. The lesson to be learned is that education produces transparency, which builds trust. After the 2002 election, and following a report by the Florida Department of State, the legislature decided to continue financially supporting voter education efforts. It also required sample ballots to be mailed or published in a newspaper prior to primary and general elections.

Although the technical voting solutions have not yet been perfectly adapted, voter opinion suggests that Florida's approach has been reasonably successful in involving local officials and the public to increase voter confidence in the process. In 2002, 66% of Florida voters said they believed that Florida's voting system "has improved significantly since 2000" [77]. After the 2000 election, only 63% of Floridians said they "think my vote counts," but by 2002 and 2004, 89% and 85%, respectively, were "confident [their] vote will count" [75, 76]. 29% of Floridians who voted in the 2004 presidential election said that their experiences were better than in 2000, while only 5% described them as worse, and the remainder said they were about the same [75].

5.3 RECOMMENDATION

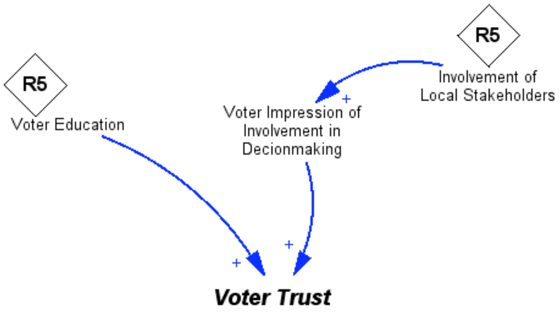
The Georgia and California case studies provide evidence that the representation of local election officials in decision-making bodies can be expected to increase public political support of the process and thereby, voter confidence. Additionally, Florida's tremendous local outreach programs significantly built voter trust in election administration. Because of HAVA's transfer of power to states, it is possible for states exclude local election officials in election administration decision-making, relegating them to simply executors of state-level decisions. We find that local expertise is invaluable to understanding the challenges of electronic voting, and therefore, we recommend:

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

Figure 13 shows this recommendation implemented in our model of voter trust. Involvement of local stakeholders in procurement and implementation decision-making creates an environment in which the voters' views are valued. Voter education initiatives like the one in

Florida also provide for public stakeholder involvement. These opportunities provide the electorate with the feeling that their voice is being heard and therefore, they begin to trust the process.

Figure 13. Recommendation 5 and the Model of Voter Trust


R5
Voter Education
R5
Involvement of Local Stakeholders
+
Voter Impression of Involvement in Decionmaking
+
+
Voter Trust

5.4 IMPLEMENTATION

The California case study is a good example of an implementation challenge. The state was forced to make cuts in representation among the various stakeholders in order to have a workable HAVA committee. The inclusion of special interest groups was intended to build support and trust in the electorate, but the exclusion of local election officials created a larger implementation challenge. The local expertise in election administration is valuable knowledge on which to base the future of electronic voting. Removing or limiting local election officials on HAVA committees is detrimental to smooth execution on Election Day.

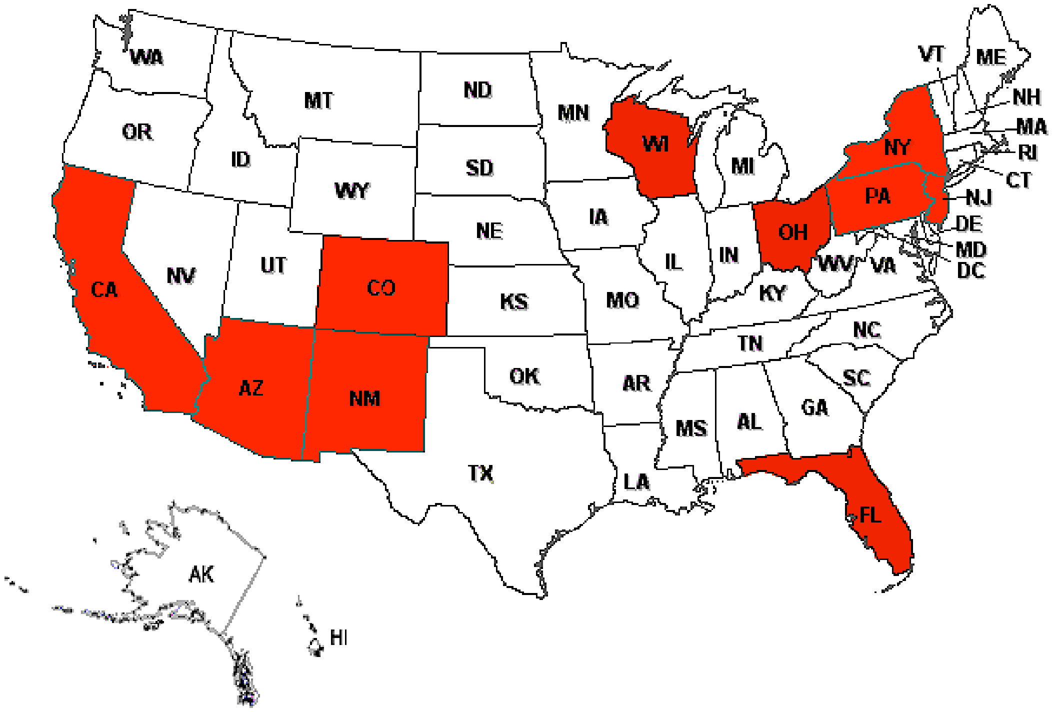
Because HAVA implementation is ongoing, several states have already selected voting technologies and machines using their HAVA funds. However, there is still room for local election official input into solving problems. For example, local election officials are best suited to concentrate on emerging poll-worker problems. In the 2006 election in Denver, more than 2 hour waits and software glitches prevented many from voting [78]. To analyze the problems, Denver is conducting five public meetings. One meeting focused on the problems that poll workers, often retirees getting paid $100 for a 14-hour day, face in conducting elections [79]. These are precisely the types of problems where knowledge of the electorate is crucial to decision-making.

6.0 CONCLUSION

The 2000 election presented a unique window of opportunity to pass significant election reform in the US. HAVA and other actions at the state level attempted to take advantage of this window, but the reforms are not comprehensive. Implementation has been incomplete, leading to the continuation of significant problems in the 2004 presidential election. We believe that problems in the 2008 election have the potential to seriously damage public perception of the voting process. Therefore, we urge that our recommendations be implemented before the next election.

While many provisions of HAVA have indeed been improvements to the voting system, the current voting system framework is insufficient to create a secure and trusted electronic voting system. Currently 10 states face election-system litigation, as shown in red in Figure 14 [80]. This fact reflects the deficiencies in HAVA and its implementation.

Figure 14. Ongoing Election-System Lawsuits Against States



Our consideration of the factors that make an electronic voting system into a secure and trusted voting system has identified five deficiencies in the current process. For each deficiency we propose a policy that, if enacted, should improve both voting system security and trust.

The deficiencies we have identified in this report include:

- **Weak technical standards**, leading to insecurity and poor system performance;

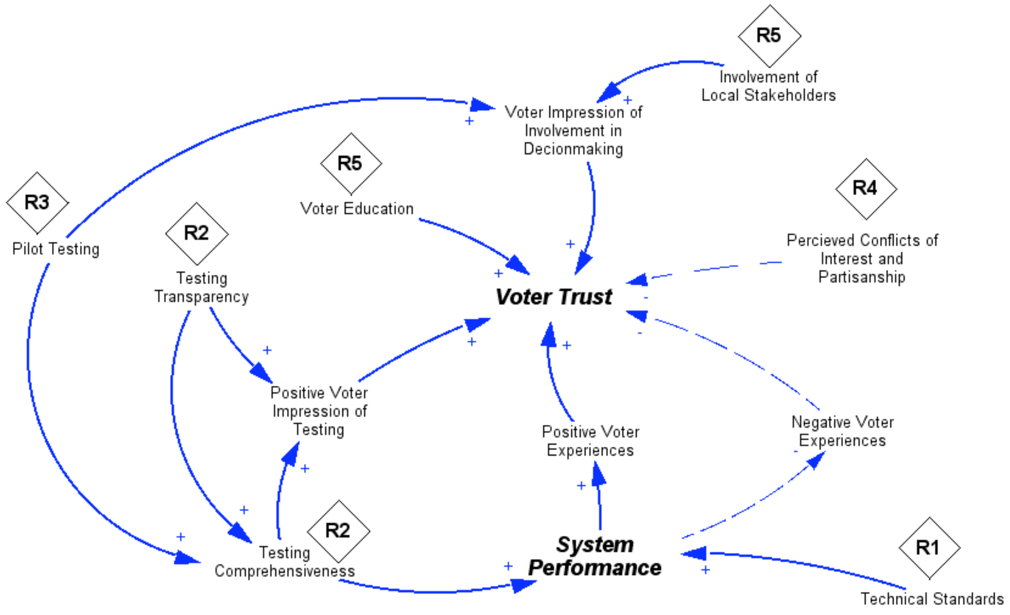
- A **weak testing system** that does little to identify insecurities or increase voter confidence in electronic voting systems;

- A **non-comprehensive testing system** that fails to identify user problems prior to wide-scale implementation, and misses the opportunity to demonstrate new technologies to the public;

- **Lack of legislation or voluntary action to prevent political and financial conflicts of interest** in the way electronic voting systems are chosen, procured, deployed, and used; and

- **Weak engagement of local interests** in the decisionmaking and procurement processes, in addition to voter education and election implementation.

Figure 15. Model of Voter Trust with Policies Implemented


R5
Involvement of Local Stakeholders
Voter Impression of Involvement in Decionmaking
R5
Voter Education
R3
Pilot Testing
R2
Testing Transparency
R4
Percieved Conflicts of Interest and Partisanship
Voter Trust
Positive Voter Impression of Testing
Positive Voter Experiences
Negative Voter Experiences
R2
Testing Comprehensiveness
System Performance
R1
Technical Standards

The evidence we have presented shows that each of these problems has serious implications for system security and system trust. Figure 15 shows how our recommendations can be implemented to improve system security and build voter confidence in electronic voting systems. Each of these policies is aimed at building trust, either indirectly by improving system security itself, or directly by improving voter perceptions of the testing and decisionmaking processes. These recommendations are:

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.

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.

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.

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.

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

Implementation of these recommendations will require careful navigation in order to overcome some concentrated political interests. Enacting effective election reform will be difficult, but the potential increases in credibility of election results, voter confidence, and greater enfranchisement are significant. Highly publicized voting system failures in two consecutive national elections, including security failures in electronic voting machines, have already seriously damaged the public perception of the voting process. At worst, continuing this trend could lead to widespread distrust of the voting system and *de facto* disenfranchisement. We therefore urge that state and federal decisionmakers move to implement our recommendations before the 2008 election.

APPENDIX A. THE ELECTORAL PROCESS

In order to understand the context for electronic voting, it is relevant to look at the overall electoral process to review its components and develop a sense of its scale. The content of this section is based on [8].

The process begins with **voter registration**, which establishes a citizen's eligibility to vote. It considers both the procedure for registration and the maintainability of the list of eligible voters. Next, there is **precinct definition** when election authorities determine a precinct's boundaries. Precinct definitions are reasonably stable, but may be subject to revision under voter's migration (among other factors).

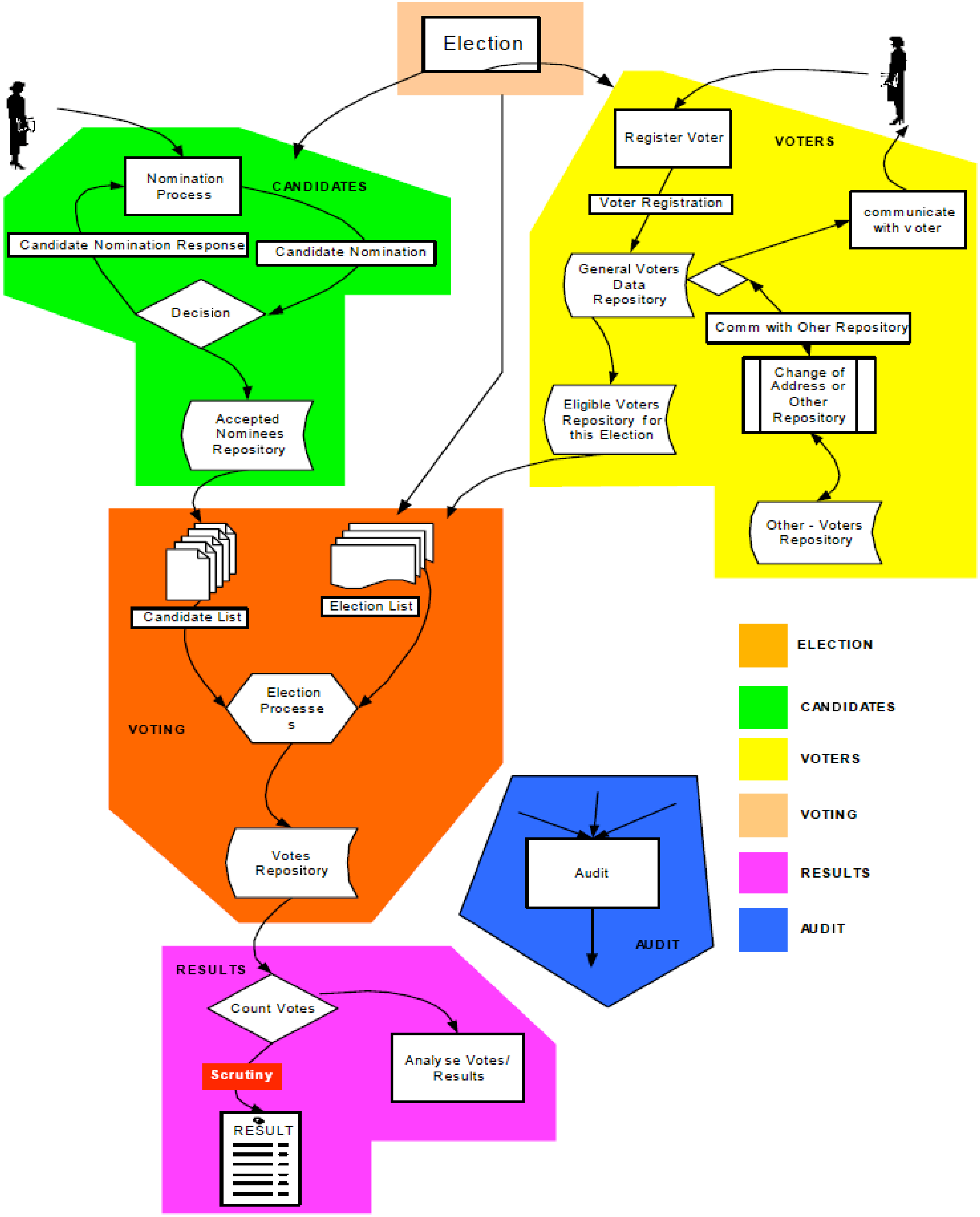
Ballots are created to indicate the contests at stake during **ballot definition**. The order that contests and propositions are placed on the ballot is dictated by each state. This process incorporates the previously defined precinct boundaries, which are further subdivided into specific geographical districts in a complex management process. The end result is expected to be a clear and usable ballot, which would entitle voters to express their preferences without confusion or difficulty.

In order to cast a ballot, each individual must go through **voter authentication** in order to prove his or her identity. This identification procedure may be enforced in different ways according to local laws. **Ballot provisioning** is needed to ensure that each voter properly receives the correct ballot on which to vote. It has to be fully accessible in terms of language and incapacity considerations so that he or she can mark the ballot to express his or her intent for that election.

There are three types of voting: **precinct voting**, for votes expressed in person during Election Day; **absentee voting**, for votes previously submitted to any local jurisdiction by mail; and **early voting**, for voters casing ballots in person in a designated location, but before Election Day.

The first round of vote counting is referred to as **initial tabulation**, which also sets the basis for potential challenges (*e.g.*,. recounts and audits). This is done by first sealing the voting machines and then calculating totals for the polling location and its precincts. This leads to the **final tabulation** which considers all valid votes from all the polled precincts. This takes place after Election Day. If anomalies are found (*e.g.*, someone challenges the outcome of the election), then a **contested election** occurs. This normally involves allegations of fraud or misconduct on the part of any of the involved parties and has to be analyzed in order to determine the actions needed to solve the allegations. An audit takes place at different levels with special concern for voter privacy and may entail a recount. The final stage is where a designated official confirms the final vote totals for each candidate. This is known as **certification** and has to take place within a specific time frame. Figure 16 provides a pictorial representation of the electoral process.

Figure 16. Flow of the Electoral Process[81]



In 2002, there were 206 million individuals of voting age and 156 million were registered to vote. For that year's election, 80 million ballots were collected among approximately 9,500 voting jurisdictions and 185,000 precincts. Election Day involved 800,000 voting machines and 1.4 million poll workers for assistance and supervision. In sum, states spend $1 billion per year on elections.

APPENDIX B. ELECTRONIC VOTING AND HAVA

Pre-HAVA History

In July 1984, with Congressional appropriations, the Federal Election Commission (FEC) began development of voluntary voting system standards (VSS) for computer-based systems [82]. In January 1990, the FEC published the first national performance and test standards. States could choose whether or not to adopt the standards as well as whether to employ more stringent standards. The VSS "specify general performance criteria, as well as detailed test criteria" [82]. The FEC also developed a three-layer testing and certification scheme that is discussed in chapter three of this report.

In 1997, the FEC began a process to update the VSS by first analyzing areas requiring improvement and then updating the actual standards [28]. They were heavily reprimanded by the General Accounting Office for failing to maintain the standards as technology changed [28]. By April 30, 2002, the FEC approved the 2002 Voting Systems Standards. The VSS was structured into two volumes: the first addressed performance standards and minimum functional capabilities and the second addressed testing [42].

HAVA and the 2005 Voluntary Voting Standard Guidelines

In 2002 HAVA established the first mandatory minimum requirements for voting systems used in federal elections effective January 1, 2006 [1]. HAVA also authorized payments to the states to carry out its directive to establish a compliant voting system including a demand to discontinue use of the punch card and lever voting systems [1]. It also established the Election Assistance Commission (EAC) whose duty was to "provide for the testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories" [1]. Despite renewed funding and considerable public interest in making progress prior to the 2006 federal elections, the EAC has not completed any of its statutory requirements on time [5].

HAVA also implemented the Technical Guidelines Development Committee (TGDC) which was to consist of representatives from numerous standards organizations that would be tasked with assisting in developing new voluntary guidelines to help interpret the mandatory requirements [1]. The Voluntary Voting System Guidelines (VVSG) were supposed to be published by January 1, 2004 [1]. They were actually published on December 13, 2005 and would not take effect until December 2007 [42]. All previous VSS will become obsolete at that time. However, in the rush to produce the VVSG by the statutory deadline, many of the public criticisms of the 1990 and 2002 standards are uncorrected in the 2005 VVSG [10].

Part of the HAVA agenda also turned over accreditation of testing agencies from the National Association of State Election Directors (NASED) to the National Institute of Standards and Technology [1]. Laboratories that are currently accredited by the NASED will be able to continue to act as Independent Testing Authorities until June 2008[7]. The EAC is currently holding public meetings on the accreditation process and has published the Draft Voting System Testing Laboratory Manual. It is hopeful that the final testing guidelines will be completed such that electronic voting machines can be re-certified prior to the 2008 federal elections.

APPENDIX C. MAJOR COMPONENTS OF DRE MACHINES

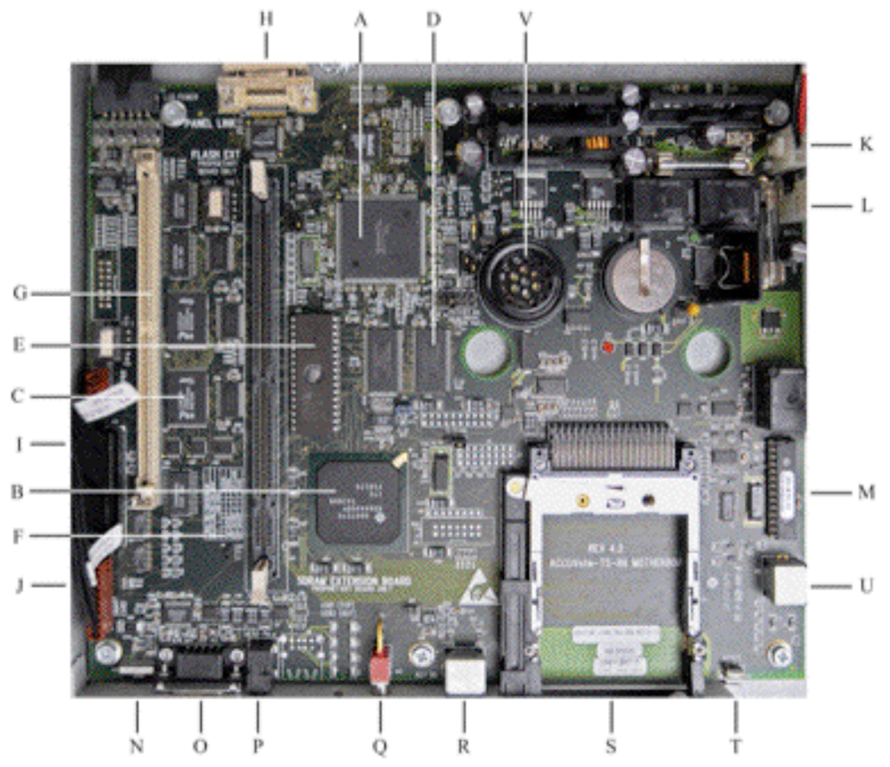
The information in this appendix is based on [25].

The major components of a DRE machine strongly resemble those of a personal computer; they include a motherboard, input (keyboard and smartcard reader), and output (touch screen). On the motherboard, there is small amount of permanent memory, larger removable memory (either flash memory cards or PCMCIA RAM chips), microprocessor, and an Erasable-Programmable ROM (EPROM) chip. During the operation, the microprocessor executes commands (Operating System and Ballot Management Software) stored on the EPROM. Figure 17 below, is the motherboard of Diebold's AccuVote TS Machine. This motherboard is representative of those found in other DRE machines.

Theses primary components are highlighted in the figure:

(A) Hitachi Branded Microprocessor
(B) Windows CE Intelligent Peripheral Controller
(C) Two 8 MB Flash Memory Chips
(D) Two 16 MB SDRAM Chips
(E) Socketed 128 KB EPROM Chip

Figure 17. AccuVote TS Motherboard [25]



APPENDIX D. RISKS IDENTIFIED BY COMPUWARE

The CompuWare report[11] commissioned by the State of Ohio found the following risks.

Code Risks

Table 1. Diebold Code Risks as Evaluated by CompuWare

	Risk		
	Likelihood	Impact	Level
The Diebold AccuVote-TS and GEMS contain additional third party components. Although the software is included in the AccuVote-TS, Diebold does not maintain these third party components. There is a risk that a security flaw in these third party products could be inadvertently introduced and cause disruption of the election process.	Low	High	Low
There is a risk that an unauthorized person could learn the PIN number of "1111" on the current version of software and gain access to the supervisor functions on the machine using any supervisor card.	High	High	High
There is a risk that the information on a smart card could be deciphered. No encryption is used in protecting the contents of a smart card. More powerful tools may exist allowing cracking of the smart cards' contents.	Medium	Medium	Medium
Data is not encrypted when transmitted over a data link. There is a risk that unencrypted data can be intercepted when transmitted over the data link.	Low	Medium	Low

Table 2. Election Systems & Software (ES&S) Code Risks as Evaluated by CompuWare

	Risk		
	Likelihood	Impact	Level
Transfer of election results is possible via modem and the ES&S "communications package." No encryption is used during the actual transmission of the data stream. There is a risk that an unauthorized person could intercept and view election data.	Low	Medium	Low
The iVotronic uses a physical device (PEB) plus two hardcoded passwords to limit access to supervisory functions. There is a risk that an unauthorized person with knowledge of these passwords might access supervisory functions on the iVotronic.	Medium	High	Medium
One user-set supervisor password is available to protect selected iVotronic functions. The password can be disabled when the election is setup on the election management software. There is a risk that due to the disabling of the supervisor password, an unauthorized person might access supervisory functions on the iVotronic.	Medium	High	Medium

Table 3. Hart-InterCivic Code Risks as Evaluated by CompuWare

	Risk		
	Likelihood	**Impact**	**Level**
Hart does not use encryption to protect data on the eSlate 3000 and JBC. There is a risk that an unauthorized person can access ballot definitions and cast vote records on the JBC.	Low	Medium	Low
The Hart eSlate 3000 and JBC do not use a supervisory mode but do optionally provide passwords. There is a risk that an unauthorized person could gain access to supervisor functions in the JBC.	Medium	High	Medium

Table 4. Sequoia Code Risks as Evaluated by CompuWare

	Risk		
	Likelihood	**Impact**	**Level**
The ballot definition and cast votes are not encrypted. There is a risk that an unauthorized person might access or modify the ballot definition and cast vote records.	Low	Medium	Low
Data stored on the PCMCIA card is not encrypted. There is a risk that an unauthorized person might access or modify data stored on the PCMCIA card.	Low	Medium	Low

Platform Risks

Table 5. Diebold Platform Risks as Evaluated by CompuWare

	Risk		
	Likelihood	**Impact**	**Level**
There is a risk that an unauthorized person might be able to create and use a counterfeit smart card to access supervisory functions or cast extra ballots.	Low	Medium	Medium
A network port is provided for loading the ballot definitions and uploading cast vote records. This should be done on a point-to-point network. There is a risk that if the AccuVote-TS is connected to an unsecured internet or intranet, the AccuVote-TS could be compromised.	High	High	High
Ports on the AccuVote-TS are covered by a locking panel. There is a risk that if the cover is unlocked during an election, the exposed ports could be used to disrupt the AccuVote-TS.	Low	High	Low
There is a risk that an unauthorized person might be able to create and use a counterfeit smart card to access supervisory functions or cast extra ballots. [In the experiment, testers were unable to create a counterfeit smart card, but the inability to do so does not indicate that it cannot be done during an election.]	Low	Medium	Medium
A network port is provided for loading the ballot definitions and downloading cast vote records. This should be done on a point-to-point network. There is a risk of a TCP hijacking attack if the AccuVote-TS is connected to an intranet or internet.	High	High	High

Table 6. ES&S Platform Risks as Evaluated by CompuWare

	Risk		
	Likelihood	**Impact**	**Level**
The iVotronic uses a physical device (PEB) plus two hardcoded passwords to limit access to supervisory functions. There is a risk that an unauthorized person with access to the supervisor PEB and knowledge of the hard-coded passwords might gain access to supervisory functions on the system.	Low	High	Low
There is a risk that an unauthorized person can gain access to the preset supervisor password.	Low	High	Low

Table 7. Hart-InterCivic Platform Risks as Evaluated by CompuWare

	Risk		
	Likelihood	**Impact**	**Level**
Access to supervisor functions, which are limited to opening and closing the polls, is controlled by physical access to the JBC and an optional password set in the BOSS election management software. There is a risk that an unauthorized person could perform supervisory functions by gaining physical access to the JBC.	High	High	High
The JBC is connected to each eSlate 3000 using a daisy-chained cable. The daisy chain connection between units is accessible to the voter and can be disrupted by disconnecting a serial port connection. Once disconnected, the JBC must be power cycled to bring the disconnected eSlates back on line. There is a risk that an unauthorized person can disconnect the daisy chain connection between the JBC and eSlate 3000, causing a disruption in voting.	High	High	High

Table 8. Sequoia Platform Risks as Evaluated by CompuWare

	Risk		
	Likelihood	**Impact**	**Level**
The AVC Edge enters supervisor mode by pressing a button on the back of the terminal without entry of any password or other access controls. There is a risk that an unauthorized person might access supervisor mode on the AVC Edge and disrupt the polling process by executing supervisor functions.	High	High	High
Polls are closed on the AVC Edge using a switch on the back of the DRE provided the preset election closing time has passed. No password is required to close the polls. A wire seal is available to cover the switch. Sequoia can provide a keyed switch for this function. There is a risk that an unauthorized person might close the polls on the AVC Edge.	High	High	High
The AVC Edge enters supervisor mode by pressing a button on the back of the terminal after the polls are closed without entry of any password or other access controls. There is a risk that an unauthorized person might access the supervisor functions and use them to disrupt the election process.	High	High	High
The PCMCIA card used on the AVC Edge is kept in a bay which can be protected by a wire seal. There is a risk that an unauthorized person might remove the PCMCIA card and disable the DRE.	Medium	High	Medium
The AVC Edge voting booth does not provide a means of locking the case. There is a risk that an unauthorized person could gain access to the AVC Edge during transportation to an election or while in storage.	High	Medium	Medium

Physical Risks

Table 9. Diebold Physical Risks as Evaluated by CompuWare

	Risk		
	Likelihood	**Impact**	**Level**
There is a risk that the PCMCIA card can be removed if the compartment is not locked. [This card can be used in a Windows PC where files can be modified or corrupted resulting in a disruption of the election process.]	Low	High	Low
GEMS uses the MS Access database to store ballot definition data and election results. There is a risk that an unauthorized person with access to the GEMS server can access the database and change ballot definition files and election results.	High	High	High
The AccuVote-TS supervisor card has an associated PIN provided by Diebold. This PIN is 1111 for all cards issued nationwide. There is a risk an unauthorized person with knowledge of this PIN will gain access to a supervisor card and use it to close the polls early.	High	High	High

Table 10. ES&S Physical Risks as Evaluated by CompuWare

	Risk		
	Likelihood	**Impact**	**Level**
A poll worker can initiate voting on the iVotronic using just the Supervisor PEB. There is a risk that an unauthorized person with access to a supervisor PEB could cast multiple ballots.	Medium	High	Medium
With a supervisor PEB and three passwords we can access any supervisory function on the iVotronic. Two of the passwords are hard-coded in the firmware and are only three characters in length. There is a risk that an unauthorized person could access the Supervisor functions (reset the machine, terminate an election early, clear or view votes) if the person has access to all passwords and supervisor PEB's.	Low	High	Low
The ES&S tally program has an "Add To" feature intended to collect data from a broken machine. This function can be executed multiple times for the same DRE with no warning, which results in over-counting of these votes. There is a risk that the election results for an iVotronic DRE might be uploaded to the UES software multiple times, and as a result votes would be over-counted.	High	High	High

Table 11. Hart Physical Risks as Evaluated by CompuWare

	Risk		
	Likelihood	**Impact**	**Level**
Access to supervisor functions, which are limited to opening and closing the polls, is controlled by physical access to the JBC and an optional password set in the BOSS election management software. No warning is provided if the user tries to close the polls before the scheduled end of the election. If the polls are closed prematurely, all eSlates attached to the JBC will be closed. There is a risk that an unauthorized person could access the JBC and close the polls prematurely.	High	High	High

Table 12. Sequoia Physical Risks as Evaluated by CompuWare

	Risk		
	Likelihood	**Impact**	**Level**
The PCMCIA card used on the AVC Edge is kept in a bay which can be protected by a wire seal. There is a risk that an unauthorized person might remove the PCMCIA card and disable the DRE.	Medium	High	Medium
Polls are closed on the AVC Edge using a switch on the back of the DRE. No password is required to close the polls. A wire seal is available to cover the switch. There is a risk that an unauthorized person might close the polls on the AVC Edge.	High	High	High
The AVC Edge enters supervisor mode by pressing a button on the back of the terminal without entry of any password or other access controls. There is a risk that an unauthorized person might access supervisor mode on the AVC Edge and disrupt the polling process by executing supervisor functions.	High	High	High

APPENDIX E. COMMITTEE CHARGE

Electronic voting systems include a large variety of systems aimed at improving the ability to conduct and administer elections more efficiently. While these systems are routinely used by private organizations and corporations to elect officers and board members, their use in public elections has always been hindered by political, technological, and procedural issues and controversies. The malfunctions that have occurred in Virginia, Maryland and Florida since the 2000 presidential election have cast greater doubt about the benefits of these systems.

Among the challenges are:

- The errors and malfunctions that have occurred;
- The fear of greater possibility of electoral fraud;
- The fears associated with the inability of humans to verify the operations occurring within the electronic machines.

The committee should review the following questions in its report:

1. What are the general technology and policy issues raised by electronic voting?

2. What are the currently available systems and those under development? What are their benefits and pitfalls?

3. Which jurisdictions have used electronic voting? What were the issues associated with each election and how were they resolved? The committee may develop case studies on some of the previous experiences with electronic voting.

4. What are the current recommendations to elections administrators for upcoming elections and how can the implementation of these recommendations increase the confidence of citizens in the electronic voting systems?

5. How can we address the technology and policy issues of electronic voting in the near future?

WORKS CITED

1. *Help America Vote Act*, U.S. Congress. 2002.

   The Help America Vote Act passed significant election reforms in response to the 2000 election. It creates the Election Assistance Commission, provides money to replace punch-card and lever systems with newer (including electronic) ones, and requires that states develop a central voter registration database.

2. Kohno, T., et al., *Analysis of an Electronic Voting System*, in *IEEE Symposium on Security and Privacy*. 2004.

   Four experts in electronic voting and computing security examined the source code for the Diebold Accuvote and found many serious flaws and vulnerabilities in its security. They state "Our analysis shows that this voting system is far below even the most minimal security standards applicable in other contexts." This system made it through federal standards/testing and state testing and certification, so it's an example of how a deeply flawed product can make it past the current system.

3. Phillips, S., *The Risks of Computerized Election Fraud: When Will Congress Rectify a 38-Year Old Problem?* Alabama Law Review, 2006. **Summer**.

   Gives an overview of how electronic systems are used in elections and details some of the irregularities that occurred in the 2004 election.

4. Fitrakis, B., S. Rosenfeld, and H. Wasserman, *Ohio's Official Non-Recount Ends Amidst New Evidence of Fraud, Theft and Judicial Contempt*, in The Free Press. Columbus, OH, December 31, 2004.

   Article on 2004 election controversy in Ohio.

5. Government Accountability Office, *Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to be Completed*, Government Accountability Office, GAO 05-965. 2005.

   A survey of recent election problems related to electronic voting. Recommends that the EAC establish a more firm timetable in establishing new testing standards and guidelines, as well as develop guidelines for lifecycle management of electronic voting systems.

6. Government Accountability Office, *Elections: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems are Under Way, But Key Activities Need to be Completed*. Government Accountability Office,, Washington, DC. 2005.

7. Government Accountability Office, *The Nation's Evolving Election System as Reflected in the November 2004 General Election*, Government Accountability Office, GAO 06-450. 2006.

   The GAO surveys HAVA implementation as of November 2004 and the extent to which reforms were reflected in the election of that year. Also gives an overview of the voting system legacy and the next years of HAVA implementation.

8. Celeste, R., D. Thornburgh, and H. Lin, eds. *Asking the Right Questions About Electronic Voting*. 2005, The National Academies Press: Washington, DC.

   The first National Research Council report to examine electronic voting, which is an ongoing research subject at NRC. This report mostly seems to frame the questions the intend to examine in future reports.

9. Science Applications International Corporation, *Diebold AccuVote-TS Voting System and Processes Risk Assessment*. Department of Budget and Management, Annapolis, MD. 2003.

   This report details the findings of an independent security review of electronic voting systems commissioned by the State of Maryland. The review found numerous security vulnerabilities. The redacted version is widely available. The original, unredacted version is available at www.bradblog.com. This website is a weblog written by Brad Friedman, an opponent of electronic voting technology and machines. He is a very biased source, but in this case, the presence of multiple versions of the same report on the Internet lead the public to be suspicious as to the "true story." Our use of this source is based on our model of public perceptions of inappropriate behavior contributing to loss of trust, whether the inappropriate behavior actually occurs.

10. Wagner, D., *Written Testimony Before the Committee on Science and Committee on House Administration*. Washington, DC. 2006.

Wagner's testimony lists a number of examples of security flaws found in ITA-certified machines. He suggests some of the reasons for these lapses and proposes reforms to the testing process to ensure that voting systems are secure.

11. CompuWare, *Direct Recording Electronic: Technical Security Assessment Report*. Ohio Secretary of State, 2003.

The CompuWare report is one of three reports that the Ohio Secretary of State commissioned to have done prior to updating its voting system. Usually these reports are confidential; but this report was accidentally released to the public. It provides detailed information concerning vulnerabilities of the machines from Diebold, Sequoia, Hart InterCivic, and ES&S vendors. This document was the only report available that allowed the group to compare and contrast machines from vendors. The results from the test were used to support the Technical chapter of the report (specific and general risks).

12. RABA Innovative Solution Cell, *Trusted Agent Report: Diebold AccuVote-TS Voting System* Columbia, MD. 2006.

Independent review of the Diebold AccuVote-TS system, commissioned by the State of Maryland, that found significant security flaws in the system.

13. Wallach, D.S., *Electronic Voting: Accuracy, Accessibility, and Fraud*, in *Democracy at Risk: The 2004 Election in Ohio*. 2005, Democratic National Committee Voting Rights Institute.

Most of this book focuses on the 2004 election in Ohio, but this chapter is more general in its criticisms of the testing process. Wallach makes a number of recommendations, including eliminating protections of proprietary information in the voting system testing process, and boosting the level of scrutiny in the testing system as a whole.

14. Shamos, M.I., *Testimony of Michael I. Shamos before the Environment, Technology, and Standards Subcommittee of the U.S. House of Representatives' Committee on Science*. Washington, D.C. 2004.

Shamos criticizes the current testing and certification system, presenting evidence of flawed systems making it through ITA testing. Shamos proposes an new testing system to be run by EAC and NIST with no protection of trade secrets or proprietary info.

15. Wagner, D., et al., *Security Analysis of the Diebold AccuBasic Interpreter*. California Secretary of State's Voting Systems Technology Assessment Advisory Board, 2006.

A report that examines the technology behind two Diebold vote tabulation systems. The researchers find that the system is susceptible to memory card attacks.

16. Brennan Center for Justice, *HAVA Implementation in the 50 States: A Summary of State Implementation Plan*. NYU School of Law, 2003.

An extended table comparing implementation of the Help America Vote Act in the 50 states. Of interest for our report is information on where purchasing is controlled (state vs. local), where education is controlled (state vs. local), and whether the state mandated a single machine.

17. Alvarez, R.M. and T. Hall, *Lessons and Trends in E-Voting: Initiatives in the US and Abroad*, in *Caltech/MIT Voting Technology Project Working Paper*. 2005.

Examines the use of pilot testing in the UK as a way of testing novel voting systems at scale. The UK experience has shown that unanticipated problems can be identified and insights can be developed by examining the use of a new technology in a scientifically designed pilot test in the real voting system.

18. Alvarez, R.M. and T. Hall, *Rational and Pluralistic Models of HAVA Implementation.* Publius, 2005. **35**(4).

Develops two case studies in which states approached HAVA implementation in different ways and with different outcomes. Georgia acted quickly, involved local officials, addressed a specific problem with rational policy analysis, and tested systems before commission to one. Its HAVA implementation is seen as successful. California had a muddled approach, little local representation, and was dominated by interest groups and political struggles between the secretary of state and others. It's HAVA implementation is seen as stalled and incomplete.

19. Election Data Services, *2006 Voting Equipment Study*. 2006.

This study provided the data on the current trends of voting machine usage in the country for federal elections. We used this data to show how DREs are dramatically increasing in use over the past 6 years.

20. Hall, J.L. *Open Source Software in E-Voting: E-Voting News and Analysis, From the Experts*. 2006. Accessed November 2006 from http://www.evoting-experts.com/index.php?p=68.

This source provided the pros and cons of open source electronic voting systems. Particularly, it provided information about past attempts to create open source voting systems that did not work and were subsequently abandoned.

21. *Open Source*. Accessed Nov. 2006 from http://www.webopedia.com/TERM/o/open_source.html.

This source gives a concise definition of Open Source Code.

22. Kitcat, J., *Source Availability and E-voting: An Advocate Recants.* Communications of the ACM, 2004. **47**(10).

Jason Kitcat, an online community consultant and former advocate of open source for voting systems, explains why there is no net benefit to making voting machine source code available to public.

23. Kilbrick, R. *VVPR Legislation*. 2006. Accessed Nov. 2006 from http://www.verifiedvoting.org/article.php?list=type&type=13.

This source details which states have legislation or requirements for VVPT mechanisms.

24. Fisher, E.A., *Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues*. CRS Report for Congress, 2003.

We used this study to provide a comprehensive overview of DREs and the technical concerns that surrounds them. This paper provided a helpful summaries of work done by major state and university groups studying electronic voting (CalTech/MIT Study group, California Task Force on E-Voting, and the John Hopkins Study).

25. Feldman, A.J., J.A. Halderman, and E.W. Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine*. Princeton University, 2006.

This paper, coupled with a published video, demonstrated several vulnerabilities of the Diebold AccuVote TS machine. The group paid particular attention to the paper’s analysis of malicious code and physical hardware.

26. Federal Election Commission, *A Plan for Implementing the FEC Voting System Standards*, Federal Election Commission, 1990.

A supplement to the Performance and Test Standards document. Proposes steps that individual states can take if they choose to adopt the Voting System Standards.

27. Federal Election Commission, *A Process for Evaluating Independent Test Authorities*, Federal Election Commission, 1990.

    Another companion to the Performance and Test Standards document. Outlines the method of evaluating and certifying the Independent Testing Authorities authorized by the 1990 guidelines to certify voting machines.

28. General Accounting Office, *Status and Use of Federal Voting Equipment Standards*, General Accounting Office, GAO 02-52. 2001.

    The GAO surveys the development of voting system standards throughout the 1990s. In addition to presenting this history, the GAO examines the testing system, concluding that the FEC has not done enough to maintain standards.

29. Associated Press, *Computer loses more than 4,000 early votes in Carteret County*, in Associated Press. November 4, 2004.

    Article reporting on a system malfunction leading to the loss of thousands of votes.

30. Local 10 News, *Broward Ballot Blunder Changes Amendment Result*, in Local 10 News Website - www.local10.com. Miami, FL, November 4, 2004.

    Details the mis-tabulation of votes by an electronic voting system.

31. Kleinberg, E., *Broward Machines Count Backward* in The Palm Beach Post. Palm Beach, FL, November 5, 2004.

    Describes another mistabulation of votes by ES&S software in FL.

32. Tinsley, A.M. and A. Spangler, *Vote Spike Blamed On Program Snafu*, in Star-Telegram. Fort Worth, TX, March 09, 2006.

    Describes a tabulation error by an ITA-certified electronic voting system.

33. Hursti, H., *Critical Security Issues with Diebold Optical Scan Design*. Black Box Voting, Inc., 2005.

    A report commissioned by a nonprofit to explore security vulnerabilities in Diebold's optical scan vote tabulation system. Hursti's findings were supported by a California report by Wagner et al.

34. Jones, D.W., *Problems with Voting Systems and the Applicable Standards. Testimony before the U.S. House of Representatives Committee on Science*. Washington, DC. 2001.

    Presents evidence of problems with the standards and testing process, focusing on software development and certification. Recommends eliminating proprietary protections of software code and investigating alternative platforms to make the system more open.

35. Jones, D.W. *The Diebold AccuVote TS Should be De-Certified*. in *USENEX Security Symposium*. 2003. Washington, DC.

    Jones has investigated this particular machine in detail and found many reasons it should not be used in elections. While an argument about a specific machine might be outside the scope of this paper, he presents evidence of significant flaws being overlooked or not covered by the current testing/standards system.

36. Mercuri, R., *The FEC Proposed Voting Systems Standard Update: A Detailed Comment by Dr. Rebecca Mercuri. Submitted to the Federal Election Commission on September 10, 2001*. 2001.

    An expert in voting systems and computer forensics offers criticism to proposed FEC guidelines. Of interest to our report are criticisms on the software/firmware, telecommunications, and security aspects of the proposed guidelines.

37. Shamos, M.I., *Testimony of Michael I. Shamos before the Election Assistance Commission on the DRAFT Procedural Manual for the Voting System and Testing Certification Program*. Washington, DC. 2006.

Shamos offers comments on proposed testing guidelines. Shamos is a state examiner of voting systems and has seen systems that have passed the federal standard even with significant flaws. He argues that the new proposed testing guidelines still do not address problems with the federal testing system.

38. National Association of State Election Directors, *General Overview for Getting a System Qualified*. National Association of State Election Directors, 2003.

Prepared by state officials to provide background and guidance regarding the federal and state testing process.

39. Election Assistance Commission, *Annual Report: Fiscal Year 2003* Election Assistance Commission, 2003.

Report documenting EAC programs and spending levels in 2003. The pilot testig program was not funded.

40. Election Assistance Commission, *Fiscal Year 2004 Annual Report*, Election Assistance Commission, 2004.

Report documenting EAC programs and spending levels in 2004. The pilot testing program was not mentioned in this document.

41. Election Assistance Commission, *Fiscal Year 2005 Annual Report*, Election Assistance Commission, 2005.

Report documenting EAC programs and spending levels in 2005. The pilot testing program was not mentioned in this document.

42. Election Assistance Commission, *Voluntary Voting System Guidelines*. Election Assistance Commission,, Washington, DC. 2005.

VVSG defines the technical standards for voting systems that are recommended by the Election Assistance Commission. They are use by ITAs to define testing methods, and they have been adopted by many states as mandatory requirements for state/local voting systems.

43. Carl Vinson Institute of Government, *Georgians Express Confidence in New Electronic Voting System*. Carl Vinson Institute of Government, University of Georgia, 2002.

This poll presents voter confidence in the voting system in Georgia, and how that confidence has changed with the implementation of some voting system reforms.

44. General Accounting Office, *Defense Pilot Programs: DOD Needs to Improve Implementation Process for Pilot Program*, General Accounting Office, GAO-03-861. 2003.

According to Alvarez and Hall, this document recommends the use of pilot testing in the development of most government projects when possible. Used as cited in R. Michael Alvarez and Thad E. Hall, “Lessons and Trends in E-Voting: Initiatives in the US and Abroad” (Caltech/MIT Voting Technology Project Working Paper 38, 2005)

45. Nagourney, A., *Democrats Take House*, in The New York Times. New York, NY, November 8, 2006.

Article on the Crisis in Public Confidence that caused the Democratic Sweep in the 2006 Election.

46. Hamilton, A., *Federalist Paper No. 78: The Judiciary Department*. 1788.

This Federalist Paper discusses the necessary political independence of the judiciary branch.

47. *U.S. Code, Title 5, Section 7323*, U.S. Congress.

This section of the US Code covers the prohibitions on political activity for certain members of the executive branch.

48. *U.S. Code, Title 5, Appendix*, U.S. Congress.

This section of the US Code encompasses the act which required more transparency in financial conflicts of interest among government officials.

49. *U.S. Code, Title 28, Section 455*, U.S. Congress.

This section of US Code covers the legal responsibilities of judges to disqualify or recuse themselves from proceedings.

50. *Open Secrets Donor Lookup*. Accessed November 2006 at http://www.opensecrets.org.

This Database compiles all soft money donations as report to the FEC by organizations.

51. Warner, M., *Machine Politics in the Digital Age*, in The New York Times. New York, NY, November 9, 2003.

Article on Diebold's partisan leanings.

52. Smyth, J.C., *Voting machine short list is delayed Ohio judge says bidder didn't get fair treatment*, in Plain Dealer. Cleveland, OH, August 16, 2003.

Article on Ohio's search for a HAVA-compliant voting system.

53. Rosenfeld, S. and H. Wasserman, *Ohio Attorney General Sues Election Protection Legal Team*, in The Free Press. Columbus, OH, January 19, 2005.

Article on 2004 election controversy in Ohio.

54. Alvarez, R.M., T.E. Hall, and M. Llewelyn, *Who Should Run Our Elections? Public Opinion About Election Governance In The United States.* Caltech/MIT Voting Technology Project Working Paper 47, 2006.

This is a paper that surveys the public on what they believe is an ideal election administration scheme.

55. Niquette, M., *Blackwell under Fire*, in Columbus Dispatch. Columbus, OH, January 8, 2005.

Article on Kenneth's Blackwell's conflict of interest.

56. Stuckey, T., *State to go ahead with purchase of touch-screen voting machines*, in Associated Press State and Local Wire. September 25, 2003.

Article on Maryland's electronic voting machine process.

57. Associated Press, *Gov. seeks probe of lobbyist with competing ties on voting machines*, in Associated Press State and Local Wire. September 27, 2003.

Article on potential conflicts of interest.

58. Smyth, J.C., *Ohio replaces voting machine reviewer; Company has financial interest in manufacturer*, in Plain Dealer. Columbus, OH, September 30, 2003.

Article on potential conflicts of interest.

59. Associated Press, *Lobbyist says Ethics Commission finds no violations*, in Associated Press State and Local Wire. November 7, 2003.

Article on conflicts of interest.

60. Stuckey, T., *Trial begins in challenge to electronic voting machines*, in Associated Press State and Local Wire. August 25, 2003.

Article on Maryland opposition to security of electronic voting machines.

61. Honawar, V., *Voting machine lawsuit rejected*, in The Maryland Gazette. Annapolis, MD, September 4, 2004.

Article on progress of Maryland lawsuit that would prevent use of electronic voting machines.

62. Kaper, S., *Group against e-voting goes to Court of Appeals*, in The Capital. Annapolis, MD, September 4, 2004.

Article on progress of Maryland lawsuit that would prevent use of electronic voting machines.

63. Associated Press, *Report criticized elections administration*, in Associated Press State and Local Wire. October 11, 2004.

Article on Linda Lamone controversy.

64. *Senator Chuck Hagel Official Biography*. 2006. Accessed November 2006 from hagel.senate.gov.

Sen. Hagel's website confirms information about his past employment.

65. Thompson, J., *Nelson still wealthiest lawmaker but if Ricketts wins Senate race, he would top Midlands money list: Who's worth the most?*, in Omaha World Herald. Omaha, NE, June 13, 2006.

Article on Hagel's potential financial conflicts of interest.

66. Kotok, C.D., *Officials trying to avoid problems*, in Omaha World Herald. Omaha, NE, November 7, 2006.

Article on financial disclosures of member of Congress.

67. *Voter Confidence and Increased Accessibility Act of 2005*, U.S. Congress. 2005.

One of up to nine new bills aimed at amending HAVA. Particularly, this strengthens legislative protections against conflict of interest.

68. *Bush v. Gore*, U.S. Supreme Court. 2000.

Landmark Supreme Court Case regarding contest 2000 Florida election results and holding that equal protection clause was violated in Florida.

69. Hocheiser, H., et al., *The Need for Usability of Electronic Voting Systems: Questions for Voters and Policy Maker*. 2005.

This paper was submitted to the NRC Computer Science and Telecommunications Board as part of their project "A Framework for Understanding Electronic Voting". It deals mostly with the requirements for the user interface of electronic voting systems.

70. Cox, C., *The 2000 Election: A Wake-Up Call For Reform and Change. Report to the Governor and Members of the General Assembly*. Georgia Secretary of State, 2001.

This is the Georgia Secretary of State's assessment of the need for radical change in Georgia's election administration procedures with particular emphasis on correcting residual voting rate deficiencies. She is a partisan, elected Secretary of State.

71. Katz, E. and R. Bolin, *Electronic Voting Machines and the Standards-Setting Process.* Journal of Internet Law, 2004.

Detailed paper regarding the history of the Voluntary System Standards for voting, both pre-HAVA and post-HAVA. Also submitted as a White Paper to National Research Council for inclusion in Richard Celeste, Dick Thornburgh, and Herbert Lin, Editors, Committee on a Framework for Understanding Electronic Voting, National Research Council. Asking the Right Questions about Electronic Voting, 2005. 7.

72. Office of the Secretary of State (California), *De-Certification and Withdrawal of Approval of Certain DRE Voting Systems and Conditional Approval of the Use of Certain DRE Voting Systems*. Sacramento, CA. 2004.

Statement of the Secretary of State Kevin Shelley detailed his de-certification announcement.

73. DiCamillo, M. and M. Field, *Voters not very confident about the state's new electronic voting systems. Many foresee voting problems in other states that could make presidential election results suspect.* Field Research Corporation, San Francisco, CA. 2004.

A poll that measures Californians' impressions of new voting systems, including electronic voting systems.

74. MacManus, S.A., *Implementing HAVA's Voter Education Requirement: A Crisis and a Federal Mandate Improve State-Local Cooperation in Florida.* Publius, 2005. **35**(4).

Detailed study of Florida's election reforms since the 2000 presidential election, including HAVA implementation and special emphasis on voter education efforts, which are judged as effective motives for voter confidence and participation.

75. Collins Center for Public Policy Inc., *2004 Voter Satisfaction Study*. Collins Center for Public Policy,, Tallahassee, FL. 2004.

A survey conducted by phone asking about the voters' experience on the election day 2004.

76. Collins Center for Public Policy Inc. and James Madison Institute, *2002 Voter Satisfaction Study: State of Florida* Collins Center for Public Policy, Inc., and James Madison Institute, Tallahassee, FL. 2002.

A survey conducted by phone about the voters' experience on the election day.

77. *Polling the Nations*. Accessed October 2006 at http://poll.orspub.com.libproxy.mit.edu/search.php.

This database contains a compilation of polls and surveys performed by research and media organizations. We used it specifically for a poll done by Fox Broadcasting in 2002 which asked whether Florida's election system had improved. Note that the URL listed here requires MIT certificates to access.

78. Chacon, D.J., *Critical failures in voting*, in Rocky Mountain News. Denver, CO, November 16, 2006.

Article on Denver's problems in the elections.

79. Urbana, I. and C. Drew, *Experts Concerned as Ballot Problems Defy an Overhaul*, in The New York Times. New York, NY, November 26, 2006.

Summary article on the biggest problems around the nation centering in Sarasota County in Florida, Denver County in Colorado as well as Ohio and Pennsylvania.

80. *Voter Action*. 2006. Accessed December 2006 from www.voteraction.org.

This site has a figure that shows states with ongoing election-system-related litigation. We use the figure for the report but do not use the site as a source of information elsewhere.

81. Oasis Election and Voter Services Technical Committee, *Election Mark-Up Language (EML): e-Voting Process and Data Requirements*. Oasis, 2002.

This documet had a great flowchart of the electoral process. We used the image but not other information from the document.

82. Federal Election Commission, *Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems*, Federal Election Commission, 1990.

The original 1990 Voting System Standards document written by the Federal Election Commission. Gives minimum requirements for multiple voting system formats.