

# CRS Report for Congress

Received through the CRS Web

## **Electronic Voting Systems (DREs): Legislation in the 108<sup>th</sup> Congress**

**August 11, 2004**

Eric A. Fischer  
Senior Specialist in Science and Technology  
Resources, Science, and Industry Division

Kevin Coleman  
Analyst in American National Government  
Government and Finance Division

# Electronic Voting Systems (DREs): Legislation in the 108<sup>th</sup> Congress

## Summary

Several bills have been introduced in the 108<sup>th</sup> Congress to address issues that have been raised about the security of direct recording electronic (DRE) voting machines. Touchscreen and other DREs using computer-style displays are arguably the most versatile and voter-friendly of any current voting system. The popularity of DREs, particularly the touchscreen variety, has grown in recent years. In addition, the Help America Vote Act of 2002 (HAVA, P.L. 107 — 252), while not requiring or prohibiting the use of any specific kind of voting system, does promote the use of DREs through some of its provisions. About 30% of voters are expected to use DREs in the November 2004 election. However, there is currently some controversy about how secure DREs are from tampering. There has been some disagreement among experts about both the seriousness of the security concerns and what should be done to address them. The bills — **H.R. 2239 (Holt), S. 1980 (Graham-FL), S. 1986 (Clinton), S. 2045 (Boxer), S. 2313 (Graham-FL), H.R. 4187 (King-IA), S. 2437 (Ensign), and H.R. 4966 (Larson)** — address these concerns in various ways:

- Requiring that all voting systems produce a paper ballot that can be verified by a voter before the vote is cast (*all except S. 1986 and H.R. 4966*), or that all voting systems produce a verifiable ballot using the most accurate technology, which may or may not be paper-based (**S. 1986**).
- Requiring that voting systems used to fulfill HAVA disability requirements use a system not requiring paper that provides for voter verification and separates vote generation from vote casting — called modular voting architecture — and providing for assisted voting as an option for jurisdictions unable to meet the requirement (**H.R. 2239/S. 1980, S. 2045, S. 2313**).
- Providing an interim paper-based system to be supplied by the Election Assistance Commission (EAC) for states unable to meet the verification requirement (**H.R. 2239/S. 1980, S. 2045, S. 2313**).
- Requiring mandatory recounts by the EAC of a small proportion of jurisdictions in each state (**H.R. 2239/S. 1980, S. 2045, S. 2313**).
- Requiring that all voting system software be available for public inspection (“open source”), as certified by the EAC (**H.R. 2239/S. 1980, S. 2045, S. 2313**), or that states be provided with copies of the software (**H.R. 4966**).
- Prohibiting the use of wireless communication devices in voting systems, with certification by the EAC (**H.R. 2239/S. 1980, S. 1986, S. 2045, S. 2313**).
- Requiring adherence to certain security requirements (*all except S. 2437*).
- Requiring federal certification of voting systems (**S. 2313**) or applying conflict-of-interest standards to certification laboratories (**H.R. 4966**).
- Posting information in the polling place regarding the availability of state administrative complaint procedures (**H.R. 4966**).
- Requiring development by the EAC of best practices for accessibility and voter-verification (**H.R. 2239/S. 1980, S. 2045, S. 2313**).
- Moving up deadlines for complying with HAVA standards (**H.R. 2239/S. 1980, S. 2045, S. 2313**).

This report will be updated in response to legislative action on the bills discussed.

## Contents

Provisions and Issues Addressed .....	4
Voter-Verified Ballot Requirement .....	4
Interim Paper System .....	6
Voter Verification for Individuals with Disabilities and Alternative Language Needs .....	7
Appropriations for Voter-Verified Systems .....	9
Requirement for Mandatory Recounts .....	10
Requirement for Open-Source Software and Prohibition of Wireless Communications .....	12
Open-Source Software .....	12
Wireless communications .....	13
Voting System Security and Testing Requirements .....	14
Certification of Security for Voter Registration Lists .....	15
Certification of Voting Systems .....	16
Posting of Information Regarding Administrative Complaint Procedures .	17
Deadline for Compliance .....	17
Best Practices .....	17
Security Consultation Services .....	18
Report to Congress .....	19
Extension of Title I Payments .....	19
Repeal of EAC Contracting Exemption .....	19
Effective Date .....	20
Conclusion .....	20

## List of Tables

Side-by-Side Comparison of Bills in the 108 <sup>th</sup> Congress on the Security of Electronic Voting Systems .....	22
--	----

# Electronic Voting Systems (DREs): Legislation in the 108<sup>th</sup> Congress

Several bills have been introduced in the 108<sup>th</sup> Congress to address issues that have been raised about the security of direct recording electronic (DRE) voting machines. DREs are the first completely computerized voting systems.<sup>1</sup> They were introduced in the 1970s. Touchscreen and other DREs using computer-style displays are arguably the most versatile and user-friendly of any current voting system. Each machine can display ballots in different languages and for different offices, depending on voters' needs. It can also display a voter's ballot choices on a single page for review before casting the vote. Finally, a DRE can be made fully accessible for persons with disabilities, including visual impairment, and can prevent several kinds of voter error. No other kind of voting system possesses all of these features.

The popularity of DREs, particularly the touchscreen variety, has been growing, and many expect that growth to continue. The Help America Vote Act of 2002 (HAVA, P.L. 107 — 252), while not requiring or prohibiting the use of any specific kind of voting system, promotes the use of DREs through some of its provisions.<sup>2</sup> The act has encouraged the replacement of punchcard and lever machines through a buyout program; it specifically states that DREs can be used to meet the accessibility requirement of the act;<sup>3</sup> and, starting in 2007, it requires any voting system purchased with HAVA funds to meet the accessibility requirement. Also, DREs easily meet the

---

<sup>1</sup> Most DREs are produced by four companies: Diebold Election Systems (which produces the Accuvote system), Election Systems and Software (iVotronic), Sequoia Voting Systems (AVC Edge), and Hart Intercivic (eSlate). There are also several smaller companies.

<sup>2</sup> For a general discussion of HAVA, see Kevin J. Coleman and Eric A. Fischer, *Elections Reform: Overview and Issues*, CRS Report RS20898, 29 March 2004; and Congressional Research Service, *Election Reform Briefing Book: Implementation in the 108th Congress*, [<http://www.congress.gov/brbk/html/eberf1.shtml>].

<sup>3</sup> §301(a)(3), Accessibility for Individuals with Disabilities, states,

The voting system shall —

(A) be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters;

(B) satisfy the requirement of subparagraph (A) through the use of at least one direct recording electronic voting system or other voting system equipped for individuals with disabilities at each polling place; and

(C) if purchased with funds made available under title II on or after January 1, 2007, meet the voting system standards for disability access (as outlined in this paragraph).

act's requirements for prevention and correction of voter errors. About 30% of registered voters are expected to use DREs in the November 2004 election.<sup>4</sup>

However, there is currently some controversy about how secure DREs are from tampering by voters, election personnel, Internet "hackers," or even manufacturers (for a detailed discussion, see CRS Report RL32139).<sup>5</sup> The controversy stems in part from another characteristic of current DREs: The ballot itself consists of electronic records, which the voter cannot see, inside the machine. Therefore, there is no way for the voter to know if the ballot that is cast is the same as the electronic representation of it on the face of the machine.

The security of DREs and other voting systems was not a major issue in the debate leading to the enactment of HAVA.<sup>6</sup> Although the issue was discussed during at least one hearing,<sup>7</sup> it became prominent only with the publication in July 2003 of an analysis of computer code for one type of DRE.<sup>8</sup>

There has been some disagreement among experts about both the seriousness of the security concerns and what should be done to address them. While it is generally accepted that tampering is possible with any computer system, given sufficient time and resources, some experts believe that the concerns can be addressed using current practices. Others believe that significant changes are needed. Among the steps proposed are requiring the use of "open source" software code, which would be available for public inspection; the development of systems that effectively mimic electronically the observability of manually counted paper ballot systems; and the printing by DREs of document ballots where a voter could verify the choices made and that would be hand-counted if the election results were

---

<sup>4</sup> Election Data Services, "New Study Shows 50 Million Voters Will Use Electronic Voting Systems, 32 Million Still with Punch Cards in 2004," Press Release, 12 February 2004. The actual percentage may be somewhat lower, as some states, such as Ohio, have postponed deployment of DREs in light of security and other issues. About 23% of registered voters used DREs in 2002.

<sup>5</sup> For a detailed discussion, see Eric A. Fischer, *Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues*, CRS Report RL32139, 4 November 2003.

<sup>6</sup> HAVA contains no explicit security requirements for voting systems. However, it does require that a voting system have an audit capacity (a common security feature) — and that this include a permanent paper record that can be used in manual recounts (§301(a)(2)), a provision added in an amendment adopted in the Senate by unanimous consent, without debate (see Eric Fischer and Kevin Coleman, *Senate Consideration and Passage of H.R. 3295 (Dodd-McConnell)*, CRS Election Reform Briefing Book, 6 May 2002, [<http://www.congress.gov/brbk/html/eberf27.html>]).

<sup>7</sup> On 22 May 2001, the House Science Committee held a hearing on the role of standards in voting technology at which the security of DREs was discussed, among other issues (House Committee on Science, *Voting Technology Standards Act of 2001*, 107th Cong., 1st sess., 2001, H.Rept. 107 — 263).

<sup>8</sup> Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, "Analysis of an Electronic Voting System," *Johns Hopkins Information Security Institute Technical Report TR-2003-19*, July 23, 2003, [<http://avirubin.com/vote/>]. See also Fischer, *Election Reform and Electronic Voting Systems*.

contested. Some experts have called for such changes before DREs are more widely adopted. Others believe that procedural and other safeguards make DREs sufficiently safe from tampering, that use of printed paper ballots would create substantial problems that would more than outweigh any benefits, and that the controversy risks drawing attention away from the demonstrated utility of DREs in addressing known problems of access to and usability of voting systems.

Several bills have been introduced in the 108<sup>th</sup> Congress that would amend HAVA to address these and other issues in various ways. The issues these bills address and the major differences in the ways they address them are discussed below. The bills that this report covers are

- **H.R. 2239**, Voter Confidence and Increased Accessibility Act of 2003, introduced May 22, 2003, by Representative Holt (identical to **S. 1980**).
- **S. 1980**, Voter Confidence and Increased Accessibility Act of 2003, introduced December 9, 2003, by Senator Graham of Florida (identical to **H.R. 2239**).
- **S. 1986**, Protecting American Democracy Act of 2003, introduced December 9, 2003, by Senator Clinton.
- **S. 2045**, Secure and Verifiable Electronic Voting Act of 2004 (SAVE Voting Act), introduced February 2, 2004, by Senator Boxer.
- **S. 2313**, Restore Elector Confidence in Our Representative Democracy Act of 2004 (RECORD Act), introduced April 8, 2004, by Senator Graham of Florida.
- **H.R. 4187**, Know Your Vote Counts Act of 2004, introduced April 21, 2004, by Representative King of Iowa.
- **S. 2437**, Voting Integrity and Verification Act of 2004, introduced May 18, 2004, by Senator Ensign.
- **H.R. 4966**, Improving Electronic Voting Standards and Disclosure Act of 2004, introduced July 22, 2004, by Representative Larson.

The House bills were referred to the House Committee on House Administration, and the Senate bills to the Senate Committee on Rules and Administration. None of the bills has received additional committee or floor action.<sup>9</sup>

---

<sup>9</sup> However, hearings have been held at which issues addressed by the bills were discussed. On June 24, 2004, the Subcommittee on Environment, Technology, and Standards of the House Science Committee held a hearing on “Testing and Certification for Voting Equipment: How Can the Process Be Improved?” The House Committee on House Administration has held an oversight hearing on “The Election Assistance Commission and Implementation of the Help America Vote Act,” on June 17, and a hearing on “Electronic Voting System Security,” on July 7. On July 20, The Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census of the House Committee on Government Reform held a hearing on “The Science of Voting Machine Technology: Accuracy, Reliability, and Security.”

## Provisions and Issues Addressed

The bills contain a broad range of provisions concerning the verification of ballots by voters, including those with disabilities, before ballots are cast; the use of interim paper-based systems; the use of mandatory recounts; the availability of voting system software for inspection by the public or by states; prohibitions on wireless communications; security, testing, and certification requirements; posting of voter information; changes in deadlines for compliance with HAVA requirements; extension of deadlines for payments under HAVA; and other matters. Those provisions and associated issues are discussed below. This report also includes a table providing a side-by-side comparison of the provisions.

### Voter-Verified Ballot Requirement

*Voter verifiability* refers to the capability of the voter to determine that his or her ballot is cast and counted as intended. No voting system currently in use in federal elections provides true voter verifiability. However, paper-based document ballot systems (hand-counted paper ballots, punchcards, and optical scan ballots) arguably exhibit somewhat more verifiability than the nondocument systems (lever machines and DREs).

With current DREs, a voter sees a representation of the choices made on a computer screen or ballot face, but cannot see what choices the machine actually records when the vote is cast. There is no independent record of the voter's choices that the machine totals can be checked against.<sup>10</sup> Document ballots, on the other hand, permit a voter to check the actual ballot before casting it, although the voter cannot verify that the votes on the ballot were counted as the voter intended.

Many computer security experts view the lack of transparency of DREs as a significant security vulnerability, and some advocate addressing this vulnerability by requiring a paper record of the voter's choices that the voter can verify before casting the ballot. This approach is often called a voter-verified paper audit trail, or VVPAT.

HAVA currently requires that a permanent paper record be produced for the voting system and that the record be available as an official record for a recount (§301(a)(2)), but it does not require either that the paper record consist of individual ballots or that the paper record be used in recounts. HAVA also requires that the system “permit the voter to verify (in a private and independent manner) the votes selected by the voter on the ballot before the ballot is cast and counted” (§301(a)(1)(A)(i)).<sup>11</sup> However, it does not specify the method of verification.

---

<sup>10</sup> Votes are recorded in more than one location inside the machine, which can protect against certain kinds of recording and counting problems, but these are not truly independent records.

<sup>11</sup> These and most other HAVA requirements go into effect in January 2006 (see Deadline for Compliance below).

All of the bills discussed in this report except **S. 1986** and **H.R. 4966** modify HAVA to require (1) that voting systems provide voter-verification via a paper ballot that the voter can inspect before the vote is cast, (2) that voters have the opportunity to correct any errors detected before casting the ballot, and (3) that the paper ballot will be a permanent record of the vote. **S. 1986** has the same requirements except the voting system is to use “the most accurate technology,” which need not be paper-based — some alternative technologies in development show promise of providing stronger voter verification capabilities than paper-based systems.<sup>12</sup> All bills except **H.R. 4187** and **H.R. 4966** specify that the voter-verified ballot be the official record for any recounts. All except **S. 1986**, **H.R. 4187**, and **H.R. 4966** require that the voter-verified ballot system be at least as suitable for manual audit as a paper ballot-box system (presumably meaning hand-counted paper ballots). **S. 2045** and **S. 2313** also prohibit the use of thermal paper for the permanent ballot record. **H.R. 2239/S. 1980**, **S. 2045**, and **S. 2313** require voter verification beginning with the November 2004 federal election. The other bills retain the current HAVA 2006 deadline for meeting §301(a) requirements.

There are two main ways that VVPAT can be implemented. In one, the paper ballot is used for the initial count as well as being preserved for audits and recounts. This is how current document-ballot systems — hand-counted ballots, punchcards, and optical scan ballots — work. Some observers have proposed separating the vote-choice and vote-casting functions of DREs to create an analogous *single-ballot* system (also called *modular voting architecture*), but DREs do not use this method. The other approach records votes electronically within the DRE but creates a parallel paper ballot record that the voter can verify and that would be used only in audits and recounts. This *parallel-ballot* approach (also called *contemporaneous paper replica*, or CPR) is most often discussed with respect to implementation of a VVPAT for DREs.

The use of VVPAT has several potential advantages, including the following:

- Any recount would be based on an independent record that the voter had had an opportunity to verify.
- Each election could be audited, and any significant discrepancies between the electronic and paper tallies would trigger a full recount.
- If the recount were performed by hand, that would take advantage of the transparency and observability that can be associated with that approach.
- The method could help ensure voter confidence in the legitimacy of election results, since voters would know that ballots they had verified would be available for recounts.

The approach also has potential disadvantages, including the following:

- The use of printers could substantially increase both the cost of administering an election and the risk of mechanical failure of a voting machine.

---

<sup>12</sup> See Fischer, *Election Reform and Electronic Voting Systems*.



- Since the use of VVPAT with DREs is largely untested, it is not clear to what extent it would improve security in practice and what impacts it might have on voters — it may make voting more complicated and time-consuming by requiring extra steps.
- Hand counting of the paper ballots would be time-consuming and arguably more error-prone than machine counting; it may also provide opportunities for tampering that do not exist with nondocument systems.
- The method will not necessarily provide the level of confidence in the results of an election that proponents project, since initial counting will still be done by computers.
- While there have been several studies of the security vulnerabilities of DREs, there have been no comparable studies for paper-based or lever voting systems; such studies are necessary to determine what the relative security risks are of DREs in comparison to other kinds of voting systems.

Although HAVA does not prohibit or require any particular voting system, the accessibility requirements effectively encourage the use of DREs, given the state of current technology. Therefore, if VVPAT is deemed essential to ensure the security and integrity of DRE voting, an argument can be made that HAVA should be revised to require it. However, to the extent that the need for VVPAT is not settled, and that requiring it might stifle innovation, and given the focus of HAVA on leaving specifics of implementation to the states, it could be argued that the decision of whether to implement VVPAT is best left to the states. Most observers appear to agree that widespread implementation of VVPAT for the November 2004 election is not feasible. Among the roughly 30 states expected to use DREs in that election,<sup>13</sup> only Nevada is requiring VVPAT for all machines in the 2004 election.<sup>14</sup> However, California requires either VVPAT or a set of other security requirements.<sup>15</sup>

## Interim Paper System

**H.R. 2239/S. 1980, S. 2045, and S. 2313** require that if a state certifies that it cannot comply with HAVA §301 requirements (as modified by these bills) by November 2004, the Election Assistance Commission (EAC) will provide the state with an interim paper-based voting system that the EAC will deem to comply with the requirements for that election. **S. 2045** includes a deadline of 1 July 2004 for states to certify that they cannot comply, and requires that the EAC reimburse jurisdictions for the costs of implementing the paper system. **S. 2313** provides for reimbursement and further stipulates that the interim system provision will apply also

---

<sup>13</sup> This estimate is based on data received from the Election Reform Information Project [<http://www.electionline.org>] and Election Data Services [<http://www.electiondataservices.com>] in March 2004.

<sup>14</sup> Nevada uses the Sequoia AVC Edge and will be using a VVPAT printer developed by Sequoia and certified for use with that system.

<sup>15</sup> See California Secretary of State Kevin Shelley, “Voting Systems,” [[http://www.ss.ca.gov/elections/elections\\_vs.html](http://www.ss.ca.gov/elections/elections_vs.html)],

for federal elections held in 2005. The bills also require that any state receiving a title I payment to replace voting systems and requesting an extension of the deadline for replacement to 2006 will use a paper-based voting system for the November 2004 election. However, **S. 2313** also permits states required to use an interim paper system to apply for a waiver if compliance is “technologically impossible.”

The paper system is to be “based on paper systems in use in the jurisdiction, if any.” **H.R. 2239/S. 1980** stipulate that the state will “receive” the system at EAC expense. It is not clear whether the interim system will be chosen by the state or by the EAC. **S. 2045** and **S. 2313** stipulate that the state will “use” the required system with costs reimbursed by the EAC. Presumably, this means that the state will choose the system.

The four bills also require that whatever system is used “shall be deemed compliant” by the EAC with HAVA requirements. Under HAVA, the EAC currently has no role in determining compliance with the requirements of the act. However, it is responsible for voluntary certification of voting systems, but by laboratories that it has accredited, not by the EAC itself. It is not clear whether the language in these bills significantly expands the authority of the EAC, or, alternatively, if compliance of any paper-based system a state chooses is automatic.

It is not clear what the cost of this provision would be, as it would depend on how many states would require interim paper systems. It would presumably include at a minimum any jurisdictions that were intending to use lever machines in the November 2004 election, as well as states with DRE systems that could not modify them to include VVPAT for that election. More than 30 states are expected to use either lever machines or DREs or both in at least some jurisdictions (roughly 75 — 80,000 precincts) in 2004.<sup>16</sup>

## **Voter Verification for Individuals with Disabilities and Alternative Language Needs**

HAVA requires that voting systems “be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters” (§301(a)(3)). It requires that there be at least one accessible system in each polling place starting in 2006, and that any voting systems purchased with HAVA title II funds starting in 2007 be fully accessible. It further states that properly equipped DREs will meet the accessibility requirement. HAVA also requires that voting systems provide alternative-language accessibility, pursuant to the requirements of the Voting Rights Act (42 U.S.C. 1973aa-1a).

DREs can provide improved accessibility in several ways. They include magnified ballots for the vision-impaired; audio ballots for blind voters and,

---

<sup>16</sup> This estimate is based on data received from the Election Reform Information Project [<http://www.electionline.org>], March 2004.

potentially, voters whose primary language is unwritten, or English speakers with substantial reading difficulty; and special interfaces for physically challenged voters.

Four of the bills require that HAVA accessibility requirements be met through use of modular voting architecture that does not require the use of paper (**H.R. 2239/S. 1980, S. 2045**) or does not require the voter to “view or handle paper” (**S. 2313**). Those bills also move the deadline for meeting accessibility requirements from 2006 to the November 2004 federal election (they move the 2007 deadline for all new machines purchased with title II funds ahead one year, to 2006). They require that jurisdictions unable to comply with this requirement and using an interim paper-ballot system provide disabled voters both the option of voting with that system with assistance from another person, as provided for by the Voting Rights Act (42 U.S.C. 1973aa-6), and the option to use another system providing for disability access, if such a system is available. The bills therefore appear to provide an interim exemption for jurisdictions from providing for voter-verifiability for disabled persons by the November 2004 election, as required for other voters. What effect this exemption might have on voting by disabled persons in 2004 is not clear, especially given the requirement in the bill that all jurisdictions use VVPAT or paper-based voting systems in that election. For example, a jurisdiction that had planned to replace a punchcard system with DREs before November 2004 might delay implementation and rely on punchcards for 2004 rather than attempting to add VVPAT to the system. In such a case, assisted voting would be the only option for blind voters in the election.

**S. 1986** requires that the method of verification used guarantee accessibility for persons with disabilities and alternative language needs, but does not specify a particular method (see above). A memorandum opinion from the U.S. Department of Justice states that electronic voting systems that produce voter-verifiable paper ballots are consistent with both HAVA and the Americans with Disabilities Act (P.L. 101-336) “so long as the voting system provides a similar opportunity for sight-impaired voters to verify their ballots before those ballots are finally cast.”<sup>17</sup>

VVPAT requires additional technology beyond the use of a printer to provide fully accessible voting for persons with disabilities, including the blind. The four bills requiring VVPAT for the 2004 election (**H.R. 2239/S. 1980, S. 2045, and S. 2313**) address this need by requiring use of a modular voting system for voters with disabilities (but not for other voters). With such a system, one device generates the ballot, recording it on a medium such as a memory card or paper, and another device is used to scan and verify the ballot (and presumably to cast and count it, although that could also be done by a third device).<sup>18</sup> Both devices would need an audio program and hardware that would read the ballot back to a blind voter, and other

---

<sup>17</sup> Sheldon Bradshaw, Deputy Assistant Attorney General, “Whether Certain Direct Recording Electronic Voting Systems Comply with the Help America Vote Act and the Americans with Disabilities Act,” Memorandum Opinion for the Principal Deputy Assistant Attorney General, Civil Rights Division, U.S. Department of Justice, 10 October 2003, available at [<http://www.usdoj.gov/olc/drevotingsystems.htm>].

<sup>18</sup> An optical scan voting system is a kind of modular system, with a pencil serving as the ballot-generating device, and the reader as the ballot-scanning device.

features to meet other accessibility requirements such as alternative languages. While such devices and programs exist and are in common use by persons with disabilities, only one such system appears to be certified under the federal voting systems standards.<sup>19</sup>

Concerns about accessibility have led some advocates for the blind to strongly oppose the imposition of a VVPAT requirement. Those advocates express additional concern that a VVPAT requirement would draw attention and resources away from efforts to make voting systems more accessible and to reduce the number of votes that are not counted or not cast as intended as a result of voter error stemming from poor usability of voting systems. Proponents argue, in contrast, that addressing the security issues associated with DREs is a critical need, and VVPAT is the only way it can be done effectively.

Advocates for the disabled also have expressed concerns that voting systems must not provide means of identifying which ballots were cast by disabled persons. Of the four bills requiring modular voting architecture for disabled persons, three (**H.R. 2239/S. 1980, S. 2045**) appear to eliminate the HAVA requirement that all future voting systems purchased with title II funds be accessible (§301(a)(3)(C)).<sup>20</sup> If, as a result, jurisdictions maintain a distinct voting system for persons with disabilities, it might permit such identification.

Some observers have pointed out that underlying concerns of voting accessibility advocates and VVPAT proponents are similar. A blind voter cannot know that the person providing assistance is recording the votes as the voter instructed, and VVPAT proponents argue that a voter using a DRE cannot know that the machine is recording the votes as the voter instructed. Both sides appear to agree that solutions are possible that would satisfy the needs of both, and major points of contention appear to revolve around perceived differences in the relative urgency needed to address the different concerns.

## Appropriations for Voter-Verified Systems

Two bills specifically provide funding for the required voter-verified systems. **S. 2045** appropriates (but does not specifically authorize) such sums as necessary and requires payments by the EAC to assist states in implementing the system, but not to exceed for any state the cost of adding a printer to existing systems. **S. 2313** contains

---

<sup>19</sup> Election Systems and Software has made available the AutoMARK Voter Assist Terminal, which provides accessibility and language features like a DRE but uses optical scan ballots, with the device printing the choices made by the voter onto the ballot. However, it does not appear to provide a means of independent voter verification for those voters who cannot read the marked ballot. At least one other company, Populex, has developed a modular, single-ballot system that prints a paper ballot that is read by a separate bar-code reader. A modular system using electronic “smartcards” rather than paper has been in use in Belgium for several years.

<sup>20</sup> This may be inadvertent. The bills replace the language of the subparagraph with a provision that does not include the requirement but also cites the subparagraph and moves the deadline it currently contains, as if the intention is to retain the requirement.

similar provisions but authorizes and appropriates \$150 million for the payments plus \$15 million for interim paper systems, and \$15 million for implementation, improved security, and recounts (see below for discussion of those provisions). The other bills contain no additional authorizations to fund their voter-verification provisions.

The cost of adding VVPAT capacity to DREs is difficult to estimate. Industry estimates have ranged from roughly \$500 — \$1,000 or more per machine. However, some believe that such estimates are significantly inflated. It is also difficult to estimate the number of DREs that would need to be fitted with printers. About 50,000 precincts may use DREs in 2004. On average, there are about 875 registered voters per precinct.<sup>21</sup> The number of registered voters per machine can range substantially among jurisdictions, from as low as about 100 voters to as high as 900. Some vendors recommend one DRE for every 250 — 400 voters, depending on local requirements. Thus, the total cost of adding VVPAT to all existing DREs is difficult to estimate, but could range from as low as \$45 million or less to more than \$200 million, not including operational and maintenance costs. For jurisdictions using lever machines (about 25,000 precincts), the voting system would have to be replaced. The 17 states currently using lever machines all have indicated that they plan to replace them by the end of 2005.<sup>22</sup> Almost all have received or expect to receive HAVA funds to assist in the replacement. Adding VVPAT for those jurisdictions could increase the total cost estimate for VVPAT by about 50% — \$65 — 300 million altogether under the assumptions above.

## Requirement for Mandatory Recounts

There are two major benefits generally cited for VVPAT. First, it gives the voter the opportunity to verify that the ballot that is cast is the one the voter intended to cast. Second, it provides a permanent record of such verified ballots that can be used in a recount. Voter verification is not by itself sufficient to determine that votes are counted as cast. It is possible, for example, that an optical scan reader could misread a sufficient number of ballots to change the outcome of an election. If the results are not sufficiently close or contested, a recount might not be performed. One way to address the question of verifying the results of an election is to perform automatic recounts for a sample of ballots. HAVA involves the EAC in studies of recount procedures and laws but does not involve it in the performance of recounts.

Three bills require the EAC to conduct and publish the results of mandatory, manual recounts of the voter-verified paper ballots in a small percentage of jurisdictions in each state, for every federal contest. **H.R. 2239/S. 1980** requires “surprise” recounts of one in every 200 jurisdictions. It requires the results of the recount to be treated in accordance with applicable law but permits citizens to appeal to the EAC if they do not believe the law provides “a fair remedy.” **S. 2045** requires

---

<sup>21</sup> Estimated from data tables in Election Data Services, “New Study.” The estimate is 938 using data for 2004, 826 for 2002, and 858 for 2000, for a mean of 874.

<sup>22</sup> Replacement plans are described in the state plans required for states applying for payments under title II of HAVA (see Election Reform Information Project, “HAVA Information Central,” 3 November 2003, [<http://www.electionline.org/site/docs/pdf/HAVA%20Information%20Central.pdf>]).

“unannounced” recounts. **S. 2313** requires “unannounced, random” recounts of 2% of jurisdictions. Neither of the latter two bills contains the appeal provision.

The method of implementation of the recount provisions appears to be ambiguous. The term *jurisdiction* is not defined in these bills or HAVA, but given how it is used, it likely refers to the unit of government within a state, whether county, town, or township, that administers an election. It is not clear if, under these bills, at least one jurisdiction per state will be subject to recount for each federal election, or if a straight probability rule will be used. This is an issue because the number of election jurisdictions per state varies substantially. Texas, for example, has 254 counties. It would therefore have at least one county recounted each election under **H.R. 2239/S. 1980** and **S. 2045**, which require a recount of 0.5% of jurisdictions, or 1 out of every 200, in each state. However, since there are more than 200 counties in the state, it is not clear whether 2 counties would be recounted each election (for an actual rate of 0.8%) or just one (0.4%), or if a second county would be recounted every four years on average (0.5%). In contrast, Maryland has 24 counties. It is not clear whether one county would be recounted each election (for an actual rate of 4.2%) or 1 county every eight years (0.5%). A similar ambiguity applies with respect to **S. 2313**, which requires a recount of 2% of jurisdictions in each state. These ambiguities would be substantially reduced if precincts, rather than jurisdictions, were chosen for recounts, since most states have more than 2,000 precincts.<sup>23</sup>

As a practical matter, it is not clear how the EAC would conduct a recount in every state, even on a limited basis. On average, the EAC would need to recount by hand roughly 1.4 million votes per election under the first two bills, and 5.6 million under the third. That might pose a significant logistical challenge and considerable costs. Also, it is not clear what standard of what constitutes a vote would be used with a given system. Under HAVA, each state is required to define “what constitutes a vote and what will be counted as a vote for each category of voting system used...” (§301(a)(6)). For the results of the recounts to be comparable to the original counts, the EAC would need to use the state standards. But since states are free to adopt different standards, the EAC would then need to use different standards in different states. Also, some states, such as California, already do partial recounts. It is not clear whether the EAC recount would replace such state procedures or be done in addition to them.

At least one analysis has questioned the effectiveness with which recounts of a small percentage of votes can detect irregularities. For example, in California, a recount of 1% of precincts is estimated to detect a discrepancy of 0.1% fewer than one out of four times on average for a statewide race, with far lower rates of detection for races for the House of Representatives.<sup>24</sup> No similar study has been done for a

---

<sup>23</sup> The number of precincts per state ranges from 142 for the District of Columbia to 24,726 for California, with a mean of 3,622 and a median of 2,157. The number of jurisdictions ranges from 1 (District of Columbia) to 1,859 (Wisconsin), with a mean of 188 and a median of 67 (data from Election Reform Information Project, March 2004).

<sup>24</sup> C. Andrew Neff, “Election Confidence: Comparison of Methodologies and Their Relative Effectiveness at Achieving It”, [<http://www.votehere.net/papers/ElectionConfidence.pdf>], (continued...)

nationwide recount, but it is likely that to be effective at detecting irregularities, a partial recount would need to sample a much higher percentage of jurisdictions than proposed by these bills.<sup>25</sup>

Currently, no federal executive agency counts votes in any election. The conducting of the recount by the EAC would therefore presumably constitute a new federal authority. Some observers may object that such authority is unconstitutional, or at least that it runs counter to the well-established practice, reinforced by HAVA, that states, not the federal government, administer elections.

## Requirement for Open-Source Software and Prohibition of Wireless Communications

**H.R. 2239/S. 1980, S. 2045, and S. 2313** require that the software code used in a voting system be disclosed to the EAC and made available for public inspection (*open source*), that the system contain no wireless communication devices, and that EAC-accredited laboratories certify that systems meet those requirements. **S. 1986** is similar except it does not require open-source software. **H. R. 4966** requires manufacturers of voting system software to provide updated copies of the software to states that use it, but does not require that the code be publicly disclosed. HAVA provides for voluntary certification of voting systems, but does not include requirements for software or for communications devices. Almost all software currently used in voting systems is proprietary. The federal voluntary voting systems standards (VSS) do not require open-source software and do not prohibit wireless communications.

**Open-Source Software.** Some computer security experts believe that open-source code is more secure than proprietary or closed-source code, while others believe that closed-source code can be at least as secure.<sup>26</sup> Voting systems currently in use rely on closed-source code. Some observers, particularly proponents of modular voting architecture, advocate a third approach, in which the device with which the voter initially makes choices is closed source, to facilitate innovation in improving usability and other aspects of the voting experience, and the device on which votes are cast and counted uses simple open-source code, to maximize transparency and take advantage of the security benefits of this approach.<sup>27</sup>

---

<sup>24</sup> (...continued)  
2 December 2003.

<sup>25</sup> For example, if errors occurred at five out of 100 precincts, a simple mathematical analysis predicts that recounting 1% would have a 5% chance of detecting the problem — that is, 95 out of 100 times no problem would be detected. A 5% recount would yield only a 30% chance of detection. It would be necessary to recount 8% to achieve a 50% chance of discovering one of the problem precincts. To achieve a 95% chance of detecting one problem precinct would require recounting 20%.

<sup>26</sup> See Jeffrey W. Seifert, *Computer Software and Open Source Issues: A Primer*, CRS Report RL31627, 17 December 2003.

<sup>27</sup> See Fischer, *Election Reform and Electronic Voting Systems*, for more detail.

The bills requiring open-source code would resolve the issue of which approach is more secure in favor of those advocating open source. Since the bills prohibit the use of undisclosed software in the voting system, they would appear to foreclose some benefits of the modular architecture approach as described above. Also, given that some current voting systems in widespread use employ proprietary commercial off-the-shelf (COTS) software, such as Microsoft Windows, this provision seems to require that those systems be reengineered to use other software or that they be withdrawn from the marketplace, since it is doubtful that a company providing closed-source COTS software would be willing to disclose the code. Furthermore, since a voting system using such software would not meet the requirements of HAVA as amended by these bills, it would need to be replaced by a paper-based system that did meet the requirements for the November 2004 election, even if the current system met the VVPAT requirement in the bill. In addition, HAVA defines voting system to include components other than those in the voting machine per se, such as the computer code used to define ballots and to make materials available to the voter. Such components are part of all voting systems and probably use proprietary software (operating systems, word processors, database software, and so forth) in all cases. Therefore, it is possible that all voting systems currently in use in the United States — except hand-counted paper-ballot systems where the ballot is not generated with the aid of a computer — would fail to meet the open-source requirement in the bills.

It is also not clear what impact an open-source requirement would have on the marketplace for voting systems. While it may draw in new companies that specialize in using open-source code, and provide new opportunities for innovation, it could also cause some current voting system manufacturers to withdraw from the marketplace, especially if they believed that revealing the code of their systems would substantially reduce the competitiveness of their products.<sup>28</sup> These potential problems could presumably be addressed by more precise language relating to what components of what voting systems the open-source requirement applies.

**Wireless communications.** The use of wireless communications in computer systems provides unique risks with respect to attack by hackers and therefore requires special attention with regard to security. Some observers believe that voting systems should not use wireless communications, because of those potential security risks, while others believe that such communications can be made sufficiently secure. However, any mode of electronic communication — by modem, Internet, or memory card, as well as wireless — provides potential points of attack for a voting system; but some means of communication is required. Many computer experts would argue that proper use of cryptographic methods would provide more security than prohibition of any one mode of communication, but that if wireless communication were to be prohibited, then Internet and possibly even modem communications should be as well. Nevertheless, wireless communication is

---

<sup>28</sup> If the reason for loss of competitiveness were security vulnerabilities that were revealed as a result of the disclosure, the withdrawal might be warranted, but if what would be revealed were legitimate intellectual property such as innovations in the user interface, then withdrawal might reduce the opportunity for further innovation.



arguably the least secure by far of the three, and the EAC recommends that it not be used.<sup>29</sup>

## Voting System Security and Testing Requirements

It is generally accepted that security should involve a focus on three elements: personnel, technology, and operations.<sup>30</sup> The personnel element focuses on a clear commitment by leadership, appropriate roles and responsibilities, access control, training, and accountability. The technology element focuses on the development, acquisition, and implementation of hardware and software. The operations element focuses on policies and procedures.

Both Maryland and Ohio have undertaken studies of the security of DREs.<sup>31</sup> While the studies took different approaches and examined different aspects of DRE security, they addressed aspects of the above elements, and each found concerns in whatever areas of security it examined. Those included computer software and hardware, and security policies and procedures, including personnel practices, along the supply chain from the manufacture of the machines to their use in the polling place. The studies made specific recommendations for addressing the risks and concerns identified, with many of the recommendations relating to operations and personnel.

HAVA contains no explicit requirements relating to those elements with regard to the development, manufacture, and deployment of voting systems. It does require technological security measures for state voter-registration lists (see below), and the auditability requirement for voting systems can be an important security control.

---

<sup>29</sup> Election Assistance Commission, “Issues and Shared Practices in Administration Management and Security for All Voting Systems,” 9 August 2004, [<http://www.eac.gov/bp/avs.asp>].

<sup>30</sup> National Security Agency (NSA), “Defense in Depth: A Practical Strategy for Achieving Information Assurance in Today’s Highly Networked Environments,” NSA Security Recommendation Guide, 8 June 2001, available at [<http://nsa2.www.conxion.com/support/guides/sd-1.pdf>].

<sup>31</sup> Science Applications International Corporation (SAIC), “Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes” (redacted), SAIC-6099-2003-261, 2 September 2003, [<http://www.dbm.maryland.gov/DBM%20Taxonomy/Technology/Policies%20&%20Publications/State%20Voting%20System%20Report/stateVotingSystemReport.html>]; Maryland Department of Legislative Services, “A Review of Issues Relating to the Diebold AccuVote-TS Voting System in Maryland,” January 2004, [[http://mlis.state.md.us/Other/voting\\_system/final\\_diebold.pdf](http://mlis.state.md.us/Other/voting_system/final_diebold.pdf)]; Maryland Department of Legislative Services, “Trusted Agent Report: Diebold AccuVote-TS Voting System,” prepared by RABA Technologies Innovative Solution Cell, 20 January 2004, [[http://mlis.state.md.us/Other/voting\\_system/trusted\\_agent\\_report.pdf](http://mlis.state.md.us/Other/voting_system/trusted_agent_report.pdf)]; Ohio Secretary of State, “DRE Security Assessment, Vol. 1, Computerized Voting Systems, Security Assessment: Summary of Findings and Recommendations,” prepared by InfoSENTRY, 21 November 2003, [<http://www.sos.state.oh.us/sos/hava/files/InfoSentry1.pdf>]; Ohio Secretary of State, “Direct Recording Electronic (DRE) Technical Security Assessment Report,” prepared by Compuware, 21 November 2003, [<http://www.sos.state.oh.us/sos/hava/files/compuware.pdf>].

**S. 1986** requires that voting systems adhere to security requirements at least as stringent as those for federal computer systems and requires that EAC-accredited laboratories certify that systems meet those requirements. **S. 2045** requires that, beginning with the November 2004 election, voting system manufacturers conduct background checks on programmers and developers, document the chain of custody for software, and implement security procedures and meet other requirements established by the Director of the National Institute of Standards and Technology (NIST); it also prohibits transmission of computer code for voting systems over the Internet and alteration of codes without recertification. The requirements in **S. 2313** are similar to those in **S. 2045** except the requirement for background checks is omitted, and the effective date is January 1, 2006.

**H.R. 4966** requires that manufacturers of voting system software provide the EAC with updated information about the identification of persons involved in writing the software, including information about any convictions for fraud. It also requires that a state test each voting machine used in an election, to ensure that the software is operating correctly, within 30 days before the election and at least once on election day. HAVA provides for but does not require the testing of voting systems.

**H.R. 4187** requires that the voluntary voting system guidelines required by HAVA include provisions on security of data transmission and receipt. The guidelines, to be developed by the EAC and supporting bodies, will replace the VSS, which do contain several provisions relating to this matter. HAVA establishes the VSS as the initial set of guidelines. HAVA does not direct the EAC to include any specific issues in the guidelines, although NIST is directed to provide technical support with respect to security, protection and prevention of fraud, and other matters. In the debate on the House floor before passage of the conference agreement on October 10, 2002, a colloquy<sup>32</sup> stipulated an interpretation that the guidelines specifically address the usability, accuracy, security, accessibility, and integrity of voting systems.

## **Certification of Security for Voter Registration Lists**

HAVA currently requires jurisdictions to provide “adequate technological security measures” to prevent unauthorized access to computerized state voter registration lists. **H.R. 2239/S. 1980, S. 2045, and S. 2313** require the EAC to certify the adequacy of those measures. The method by which the EAC is to perform the certification is not specified. HAVA currently gives the EAC authority to accredit laboratories that can certify voting systems (see below), but the use by states of such systems is voluntary. The provisions therefore give the EAC new authority. While the required certification may result in improved security, some may object to providing such authority to the federal government over the administration of elections by states.

---

<sup>32</sup> Congressional Record, daily ed., 148: H7842.

## Certification of Voting Systems

Under HAVA, the certification of voting systems is not a federal requirement but is voluntary. Accredited independent testing laboratories (ITAs) test computer-assisted voting system hardware and software to determine compliance with the guidelines (there are currently no federal standards for lever machines and hand-counted paper-ballot systems). Systems deemed to comply receive certification. Most states have adopted the standards or require testing against them.<sup>33</sup> However, the standards and certification process have been somewhat controversial. The VSS have been criticized for inadequately addressing usability, security, administrative procedures and practices, performance in actual use, voter registration systems, and other aspects of election administration.<sup>34</sup> Some also believe that the current system of ITAs has created bottlenecks in certifying new systems and that more certified testing laboratories are needed.<sup>35</sup> Some critics also point out that most of the weaknesses and problems found with the software and hardware used in DREs and other computer-assisted voting systems occurred in systems that had been certified by ITAs.

**S. 2313** requires states to use voting systems certified by the EAC as meeting HAVA §301 requirements. Alternatively, they may use an interim paper-ballot system or apply to the EAC for a waiver. The method by which the EAC is to perform certification is not specified. HAVA distinguishes between the guidelines (§221), which will replace the VSS, and guidance (§312), which the EAC will develop to assist states in meeting the requirements. The act does not specify what the relationship should be between the two, nor do the testing and certification provisions in §231 explicitly state the relationship of testing and certification to either the guidelines or guidance. However, a reasonable interpretation is that voting systems will be tested and certified against the guidelines, since they replace the VSS.

Some critics have expressed concerns about relationships between some organizations involved in the certification of voting systems and manufacturers.<sup>36</sup> **H.R. 4966** requires that laboratories accredited by the EAC to test and certify voting systems adhere to standards, to be established by the EAC, for avoiding financial and other conflicts of interest. HAVA currently contains no provisions relating to conflict of interest.

---

<sup>33</sup> Federal Election Commission, “Frequently Asked Questions about Voting System Standards,” 18 May 2001, available at [<http://www.fec.gov/pages/faqs/vss.htm>].

<sup>34</sup> See, for example, comments submitted on the draft revision to the VSS, available at [<http://www.fec.gov/pages/vss/comments/comments.html>], 17 September 2002. See also Fischer, *Election Reform and Electronic Voting Systems*.

<sup>35</sup> National Institute of Standards and Technology is developing a new laboratory accreditation program, as required by HAVA.

<sup>36</sup> Linda K. Harris, “Group That Called Electronic Vote Secure Got Makers’ Aid,” *The Philadelphia Inquirer*, 25 March 2004, p. A2.

## Posting of Information Regarding Administrative Complaint Procedures

HAVA requires that certain information be publicly posted at each polling place on election day, including a sample ballot, polling place hours, instructions for those required to show ID to vote, voting rights under federal and state law, and prohibitions on fraud and misrepresentation under federal and state law (§302(b)). HAVA also requires that each state receiving HAVA funds establish a program whereby persons can file a complaint regarding compliance with the title III requirements and follow specified procedures for handling the complaint (§402). However, the act does not require that information on the availability of that complaint procedure be posted. **H.R. 4966** requires that the posted voter information include the availability of §402 administrative complaint procedures for those who believe that equipment is malfunctioning or that HAVA requirements are not being followed.

## Deadline for Compliance

The deadline for compliance with most HAVA requirements is January 1, 2006. The exceptions are the provisional voting and voter information requirements of §302 and the voter identification requirements of §303, which went into effect January 1, 2004; and the accessibility requirement for new voting systems in §301, which go into effect January 1, 2007.

**H.R. 2239/S. 1980** and **S. 2045** move the deadline for all HAVA voting system requirements in §301 (as modified by these bills), from January 1, 2006, to the November 2004 federal election, and move up by one year, to January 1, 2006, the date by which all new voting systems purchased with title II funds are required to meet the act's accessibility requirements. **S. 2313** moves to the November 2004 election the deadline for meeting §301 requirements (as modified by the bill), for error correction, voter verification and auditing, provision of at least one fully accessible voting system per polling place, instruction of election officials on assistance to voters, and open source software and the prohibition on the use of wireless communications; other requirements go into effect January 1, 2006. **H.R. 4966** requires the EAC to adopt voluntary voting system guidelines regarding the software requirements in the bill by January 1, 2006; and standards on conflict of interest for accredited laboratories by the same date. Many observers believe that too little time remains before the November election for states to meet VVPAT or other new requirements, should any of these bills be enacted. Some have even expressed concerns about the ability of states to meet the current 2006 requirements under HAVA.

## Best Practices

Many issues of concern with respect to the November 2004 election might be addressed to a significant extent through improvements in practices that could be implemented before the election. They include such issues as ballot design, voter error, the accuracy of counts, and security. Several observers have suggested that a

specific set of best practices should be developed, and the EAC has issued a best practices “tool kit.”<sup>37</sup>

**H.R. 2239/S. 1980, S. 2045, and S. 2313** require the EAC to “study, test, and develop best practices to enhance accessibility and voter-verification mechanisms for disabled voters.” HAVA includes accessibility, accuracy, security, and equal opportunity among the goals for the periodic studies required under §241, and §245 requires a study of electronic voting, which may include “the appropriate security measures required and minimum standards for certification of systems or technologies in order to minimize the potential for fraud in voting.” The act does not include any provisions specifically relating to the study of voter verification for either disabled or any other voters. It does require the development of best practices in certain areas: recounts (§241(b)(13)(B)) and facilitating military and overseas voting (§242(b)).

The term best practices is often used in business and government, but is rarely well characterized. It often refers to strategies, policies, procedures, and other action-related elements that are generally accepted as being the most successful or cost-effective for meeting a specified set of goals. Unfortunately, there does not appear to be any overall agreement on how a best practice should be identified. Ideally, perhaps, it would involve a set of practices that were empirically and objectively demonstrated to be the best among various alternatives for achieving a stated set of goals. That is rarely achieved, and more often best practices are the result of a consensus process involving selected experts. Such an approach can be effective, but in the absence of empirical comparisons, there is the risk of a gap between what is generally perceived to be a best practice and what in fact would be best. Therefore, the utility of the sets of practices required by the bills would depend to a significant extent on the methods by which they were developed.

## Security Consultation Services

Few election officials are well-versed in security procedures and other controls, and HAVA contains no mechanisms to assist them in that regard. **S. 1986 and S. 2313** require NIST to provide security consultation services to state and local jurisdictions and authorize \$2 million per year through FY2006 for that purpose. NIST currently provides assistance to federal agencies in improving their information security programs.<sup>38</sup> NIST provides some assistance to states and local governments, for example in weights and measures and computer forensics investigations.<sup>39</sup>

---

<sup>37</sup> Election Assistance Commission, “Best Practices in Administration, Management and Security in Voting Systems and Provisional Voting: A Tool Kit for Election Administrators and Stakeholders,” 9 August 2004, [<http://www.eac.gov/bp>].

<sup>38</sup> See, for example, NIST, “Program Review for Information Security Management Assistance,” 10 March 2004, [<http://prisma.nist.gov>].

<sup>39</sup> See NIST, “About Weights and Measures Division,” 4 December 2002, [[http://ts.nist.gov/ts/htdocs/230/235/owm\\_about.htm](http://ts.nist.gov/ts/htdocs/230/235/owm_about.htm)]; NIST, “National Software Reference Library (NSRL),” 30 March 2004, [<http://www.itl.nist.gov/div897/docs/nsrl.html>].

## Report to Congress

HAVA requires the EAC to report to Congress on a wide range of subjects. In addition to an annual report, periodic reports are required on a wide range of election administration topics, and specific reports are required on best practices for facilitating military and overseas voting, human factors research relating to voting, voters who register by mail, the use of Social Security information in election administration, electronic voting and the electoral process, and free absentee ballot postage.

**H.R. 2239/S. 1980** requires the EAC, in consultation with NIST, to report to Congress regarding a proposed security review and certification process for all voting systems. It also requires the Government Accountability Office (GAO) to issue a report to Congress on the operational and management systems that should be used to safeguard the security of voting systems, and a schedule for implementation. **S. 2313** requires an identical security review study as **S. 1986**, but also requires it to include a description of the voting system certification process required by §231 of HAVA. **S. 2313** also requires a similar report on operational and management systems as **S. 1986**, but requires that in addition the report examine such systems for federal elections generally and security standards for manufacturers, and that the report be done by the EAC rather than GAO.

## Extension of Title I Payments

HAVA requires that title I funds returned and unobligated as of September 1, 2003, be transferred from GSA to the EAC and be used for title II requirements payments (§104(c)(2)). All appropriated title I funds have been distributed.<sup>40</sup> The act also required that states receiving title I payments to replace punchcards and lever machines were to request a waiver by January 1, 2004, if they were unable to replace the systems before November 2, 2004 (§102(a)(3)(B)). **H.R. 2239/S. 1980** would have extended the deadline for requesting payments under title I of HAVA to November 2003; **S. 2045** extends the deadline to November 2, 2004. **S. 2313** would have extended to August 1, 2004, the waiver deadline for the punchcard and lever machine replacement program. Seven of the 30 states that received replacement funds did not apply for a waiver.<sup>41</sup>

## Repeal of EAC Contracting Exemption

HAVA (§205(e)) exempts the EAC from requirements to advertise when procuring supplies and services (41 USC 5). **H.R. 2239/S. 1980**, **S. 2045**, and **S. 2313** repeal that exemption.

---

<sup>40</sup> See EAC, “Early Money to States: GSA Statistics,” 28 July 2004, [[http://www.eac.gov/gsa\\_stats\\_early\\_money.asp](http://www.eac.gov/gsa_stats_early_money.asp)].

<sup>41</sup> Those states are Alabama, Arizona, Florida, Georgia, Maryland, Oregon, and South Carolina.

## Effective Date

**H.R. 2239/S. 1980** stipulates that provisions in the bill will take effect as if they had been included in HAVA when it was enacted, except that the repeal of the contracting exemption will be effective upon enactment of the bill. **S. 1986, H.R. 4187** and **S. 2437** are similar except they do not include the contracting provision. **S. 2045** is also similar to **H.R. 2239/S. 1980**, but also stipulates that the security requirements in the bill will apply to voting systems in use beginning November 2, 2004. **H.R. 4966** stipulates that provisions in the bill will take effect with the November 2006 federal election except as otherwise specified.

## Conclusion

The bills discussed in this report would all increase the federal role in the administration of elections, some of them substantially. HAVA does not specifically require any particular method of voting or prohibit any particular type of voting system (see for example §301(c)), nor does it give the EAC any explicit authority or operational role in the administration of elections. It leaves methods of complying with the requirements of title III to the states (§305). Federal guidelines and certification of voting systems remain voluntary under HAVA.

Several of the bills discussed in this report, in contrast, would significantly change those aspects of HAVA, by, for example, effectively prohibiting any voting system that does not use or produce a paper ballot, requiring that only EAC-certified voting systems be used or that the EAC certify the security of state computerized voter-registration lists, or requiring the EAC to perform recounts of a portion of election results in each state. While Congress has the authority to regulate federal elections, some of the proposed provisions might be subject to legal challenge.

While potential impacts of these bills, if enacted, on the implementation of HAVA are difficult to assess, there are at least four potential areas of impact: the administration of the November 2004 and subsequent elections, the costs of complying with the provisions of the bills, effects on accessibility provisions of HAVA, and potential impacts on the marketplace. These potential impacts have been discussed to some extent above and are summarized here.

- Moving up deadlines would have the potential benefit of accelerating compliance with HAVA requirements. However, to the extent that states have developed and are implementing plans in response to the current deadlines, such changes could be disruptive. Furthermore, many of the changes to HAVA requirements contained in the bills would also require significant changes to current state plans and activities. Because elections are complex to administer, such changes could have unpredictable and possibly negative effects.
- The bills could add significantly to the costs of implementing HAVA. Implementing the VVPAT provision alone could cost several hundred million dollars. Other costs are more difficult to estimate but could be substantial.

- The VVPAT requirement and related provisions could slow the adoption of DREs and therefore impede the development of fully accessible voting in the United States. However, its actual likely impact is difficult to assess. At the same time, several of the bills accelerate adoption of fully accessible voting systems by moving up deadlines for their deployment.
- If the provisions in several bills caused significant changes in the voting industry, more jurisdictions might be required to change voting systems because of withdrawal of some manufacturers from the marketplace. That could disrupt the implementation of state plans and increase costs. At the same time, however, such changes to the industry might open opportunities for innovative companies to enter the market. For example, the VVPAT requirement might increase market demand for modular-architecture, document-ballot systems in lieu of parallel-ballot DREs. That may be likely under some of the bills, given that all new voting systems would have to use modular voting architecture for disabled voters beginning in 2006. In the longer term, the VVPAT requirement could result in greater uniformity of state voting systems, with attendant benefits and risks, but it could also impede the development of new, superior approaches to voting, some of which are currently in development.<sup>42</sup>

With a short time remaining until the November 2004 election, several of the issues addressed by the bills discussed in this report may be expected to persist beyond it. Close scrutiny of the election by the media and public interest groups is anticipated. Prospects for further consideration of the provisions in these bills after the election, by the 108<sup>th</sup> or 109<sup>th</sup> Congress, is likely to depend in part on the results of that scrutiny.

---

<sup>42</sup> See Fischer, *Election Reform and Electronic Voting Systems*.



## Side-by-Side Comparison of Bills in the 108<sup>th</sup> Congress on the Security of Electronic Voting Systems

H.R. 2239/S. 1980	S. 1986	S. 2045	S. 2313	H.R. 4187	S. 2437	H.R. 4966
<b>Requirement for voter-verified ballot</b>						
Sec. 4(a) modifies §301(a)(2) of the Help America Vote Act of 2002 (HAVA) to require that voting systems produce voter-verified paper records for manual auditing that are “equivalent or superior to paper ballot box systems,” that those documents be the official record for any recount, and that voters have the option to correct errors before the ballot is cast.	Sec. 2(a) modifies §301(a)(2) to require that voting systems provide a means for a voter to verify his or her vote, that voters have the option to correct errors before the ballot is cast, and that those verified votes be the official records for any recount. Requires the use of the most accurate technology, which may or may not be paper-based.	Sec. 2(a) provisions are identical to those in <b>H.R. 2239/S. 1980</b> , but additionally prohibits the use of thermal paper for the paper record.	Sec. 2(a)(1) contains similar requirements to those in <b>S. 2045</b> .	Sec. 2(a) modifies §301(a)(2) to require that voting systems provide an auditable paper record that the voter uses to verify that votes are as intended, and provide the opportunity to correct errors before the vote is cast; and that the paper record serve as the permanent record of the votes. Sec. 2(b) prohibits removal of the paper record from the polling place other than by an election official.	Sec. 2(a) contains similar requirements to those in <b>H.R. 2239/S. 1980</b> but also requires electronic records to be “consistent” with the paper records.	no provision
<b>Voter Verification for Voters with Disabilities and Languages other than English</b>						
Sec. 4(b) requires that voting systems	Sec 2(a) requires that the voting	Sec. 2(b) and (c) contain similar	Sec. 2(b) and (c) contain similar	no provision	no provision	no provision

<b>H.R. 2239/S. 1980</b>	<b>S. 1986</b>	<b>S. 2045</b>	<b>S. 2313</b>	<b>H.R. 4187</b>	<b>S. 2437</b>	<b>H.R. 4966</b>
<p>used to fulfill the accessibility requirements of HAVA (§301(a)(3)) provide for voter verifiability of ballots through a means not requiring paper that separates the vote- generation and vote- casting functions of the voting system (known as modular voting architecture). It also provides an alternative for jurisdictions that are unable to comply with this requirement in time for the November 2004 federal election. Such jurisdictions must provide, for the disabled voter to use at his or her option, (1) a paper-ballot system that the voter can use with the help of another</p>	<p>system be accessible for voters with disabilities as required by §301(a)(3)(A) of HAVA and for voters using a language other than English as required under the Voting Rights Act.</p>	<p>requirements to those in Sec. 4(b) of <b>H.R. 2239/S. 1980.</b></p>	<p>requirements to those in Sec. 4(b) of <b>H.R. 2239/S. 1980.</b></p>			

<b>H.R. 2239/S. 1980</b>	<b>S. 1986</b>	<b>S. 2045</b>	<b>S. 2313</b>	<b>H.R. 4187</b>	<b>S. 2437</b>	<b>H.R. 4966</b>
<p>person, with election officials being instructed in the rights of such voters in that regard, and (2) a system without voter verification that meets the current HAVA accessibility requirements, except that the second option is not required until January 1, 2006.</p>						
<b>Interim Paper System</b>						
<p>Sec. 5(b) requires that if a state certifies that it cannot comply with HAVA §301 requirements by November 2004, the Election Assistance Commission (EAC) will provide the state, at EAC expense, a paper-based system that the EAC will</p>	<p>no provision</p>	<p>Sec. 4(b) contains similar requirements to those in Sec. 5(b) of <b>H.R. 2239/S. 1980</b> except it includes a certification deadline (July 1, 2004), and specifies that the EAC will reimburse jurisdictions for the costs of implementing an</p>	<p>Sec. 4(b) contains similar requirements to those in Sec. 5(b) and 3(d) of <b>S. 2045</b> except it specifically includes federal elections in 2005 as well as 2004. It also permits states required to use an interim paper system to apply for</p>	<p>no provision</p>	<p>no provision</p>	<p>no provision</p>

H.R. 2239/S. 1980	S. 1986	S. 2045	S. 2313	H.R. 4187	S. 2437	H.R. 4966
<p>deem to comply with the requirements for that election. Sec. 2(d) requires that any state receiving a title I payment to replace voting systems and requesting an extension of the deadline for replacement to 2006 will use a paper-based voting system for the November 2004 election.</p>		<p>interim paper system. Sec. 3(d) contains similar requirements to those in Sec. 2(d) of <b>H.R. 2239/S. 1980.</b></p>	<p>a waiver if compliance is “technologically impossible.”</p>			
<b>Appropriations for Voter-Verified Systems</b>						
no provision	no provision	<p>Sec. 2(d) appropriates such sums as necessary and requires payments by the EAC to assist states in implementing the required voter-verified system, but not to exceed for any state the cost of adding a printer to</p>	<p>Sec. 9 contains identical provisions to Sec. 2(d) of <b>S. 2045</b> except it authorizes and appropriates \$150 million for the payments plus \$15 million for interim paper systems and \$15 million for implementation,</p>	no provision	no provision	no provision

H.R. 2239/S. 1980	S. 1986	S. 2045	S. 2313	H.R. 4187	S. 2437	H.R. 4966
		existing systems to meet the requirement.	improved security, and recounts.			
<b>Requirement for Mandatory Recounts</b>						
Sec. 7 requires the EAC to conduct surprise recounts for each federal office in one of every 200 jurisdictions (0.5%) in each state and overseas and to publish the results. It also stipulates that the results will be treated in accordance with applicable law but permits any “citizen of the jurisdiction” to appeal to the EAC if they believe that law “does not provide a fair remedy.”	no provision	Sec. 6 contains similar requirements to those in Sec. 7 of <b>H.R. 2239/S. 1980</b> except it does not include the appeal provision.	Sec. 7 contains similar requirements to those in Sec. 7 of <b>S. 2045</b> except it requires “random” recounts of 2% of jurisdictions.	no provision	no provision	no provision
<b>Requirement for Open-Source Software and Prohibition of Wireless Communications</b>						
Sec. 4(a) requires that the software code used in a	Sec. 3 prohibits the use of wireless devices in voting	Sec. 2(a) provisions are identical to those of Sec. 4(a) of	Sec. 2(c) requirements are similar to those of	no provision	no provision	Sec. 2(a) requires manufacturers of voting system

H.R. 2239/S. 1980	S. 1986	S. 2045	S. 2313	H.R. 4187	S. 2437	H.R. 4966
voting system be disclosed to the EAC and made available for public inspection (“open source”), that the system contain no wireless communication devices, and that EAC-accredited laboratories certify that systems meet those requirements.	systems and requires that EAC-accredited laboratories certify that systems meet that requirement.	<b>H.R. 2239/S. 1980.</b>	Sec. 4(a) of <b>H.R. 2239/S. 1980.</b>			software to provide a state using the system with an updated copy of the software.
<b>Voting System Security and Testing Requirements</b>						
no provision	Sec. 3 modifies §301(a) of HAVA to require that voting systems adhere to security requirements at least as stringent as those for federal computer systems and requires that EAC-accredited laboratories certify that systems meet that requirement.	Sec. 7 requires that, beginning with the November 2004 election, voting system manufacturers conduct background checks on programmers and developers, document the chain of custody for software, and implement security procedures and meet other requirements established	Sec. 2(c) requirements are similar to those in Sec. 7 of <b>S. 2045</b> except the requirement for background checks is omitted, and the effective date is January 1, 2006.	Sec. 2(c) requires that the Voluntary Voting System Guidelines required by Sec. 221(b) of HAVA include provisions on security of data transmission and receipt.	no provision	Sec. 2(a) requires that manufacturers of voting system software provide the EAC with updated information about persons involved in writing the software, including information about any convictions for fraud. It also requires that a state test each voting machine used in an election, to ensure that the

H.R. 2239/S. 1980	S. 1986	S. 2045	S. 2313	H.R. 4187	S. 2437	H.R. 4966
		by the Director of the National Institute of Standards and Technology (NIST); also prohibits transmission of computer code for voting systems over the Internet and alteration of codes without recertification.				software is operating correctly, within 30 days before the election and at least once on election day.
<b>Certification of Security for Voter Registration Lists</b>						
Sec. 6 modifies §303(a)(3) of HAVA to require the EAC to certify the adequacy of technological security measures for computerized state voter registration lists.	no provision	Sec. 5 contains a similar requirement as Sec. 6 of <b>H.R. 2239/S. 1980</b> .	Sec. 5 is identical to Sec. 5 of <b>S. 2045</b> .	no provision	no provision	no provision
<b>Certification of Voting Systems</b>						
no separate provision, but Sec. 4(a) requires that voting system	no separate provision, but Sec. 3(a) requires that voting system	no separate provision, but Sec. 2(a) requires that voting system	Sec. 4(b) requires states to use voting systems certified by the EAC as meeting	no provision	no provision	Sec. 3(a) requires that laboratories accredited by the EAC to test and

<b>H.R. 2239/S. 1980</b>	<b>S. 1986</b>	<b>S. 2045</b>	<b>S. 2313</b>	<b>H.R. 4187</b>	<b>S. 2437</b>	<b>H.R. 4966</b>
software be certified as meeting requirements of that section.	software be certified as meeting requirements of that section. no general provision	software be certified as meeting requirements of that section. no general provision	HAVA §301 requirements, or an interim paper-ballot system, or to apply to the EAC for a waiver.			certify voting systems adhere to standards for avoiding conflicts of interest to be established by the EAC.
<b>Posting of Information Regarding Administrative Complaint Procedures</b>						
no provision	no provision	no provision	no provision	no provision	no provision	Sec. 4 requires that the information posted in the polling place under HAVA §302(b) include the availability of administrative complaint procedures required by §402 for those who believe that equipment is malfunctioning or that HAVA requirements are not being followed.
<b>Deadline for Compliance</b>						
Sec. 5(a) moves the deadline for all HAVA voting system	no provision	Sec. 4(a) is identical to Sec. 5(a) of <b>H.R. 2239/S. 1980.</b> Sec 2(b) is similar	Sec. 3 moves to November 2004 the deadline for HAVA requirements, as	no provision	no provision	Sec. 2(b) requires the EAC to adopt voluntary voting system guidelines



H.R. 2239/S. 1980	S. 1986	S. 2045	S. 2313	H.R. 4187	S. 2437	H.R. 4966
<p>requirements in §301 from January 1, 2006, to the November 2004 election.</p> <p>Section 4(b) also moves up by one year, to January 1, 2006, the date by which all new voting systems purchased under HAVA are required to meet the act's accessibility requirements.</p>		<p>to Sec. 4(b) of <b>H.R. 2239/S. 1980.</b></p>	<p>modified, for error correction (§301(a)(1)), voter verification and auditing (2), provision of at least one fully accessible voting system per polling place (3)(B), instruction of election officials on assistance to voters (8), open source software (9) and the prohibition on the use of wireless communications (10).</p>			<p>regarding the software requirements in Sec. 3(a) by January 1, 2006.</p> <p>Sec. 3(b) requires the EAC to establish standards regarding the requirements in Sec. 3(a) by January 1, 2006.</p>
<b>Best Practices</b>						
<p>Sec. 4(c) requires the EAC to “study, test, and develop best practices to enhance accessibility and voter-verification mechanisms for disabled voters.”</p>	<p>no provision</p>	<p>Sec. 2(e) requires an identical study as Sec. 4(c) of <b>H.R. 2239/S. 1980.</b></p>	<p>Sec. 8 requires an identical study as Sec. 4(c) of <b>H.R. 2239/S. 1980.</b></p>	<p>no provision</p>	<p>no provision</p>	<p>no provision</p>

H.R. 2239/S. 1980	S. 1986	S. 2045	S. 2313	H.R. 4187	S. 2437	H.R. 4966
<b>Security Consultation Services</b>						
no provision	Sec. 3(a) requires NIST, upon enactment, to provide security consultation services to state and local jurisdictions and authorizes \$2 million per year through 2006 for that purpose.	no provision	Sec. 10(2) contains a similar requirement to Sec. 3(a) of <b>S. 1986</b> .	no provision	no provision	no provision
<b>Report to Congress</b>						
no provision	Sec. 3(a) requires the EAC, in consultation with NIST, to report to Congress within six months after enactment regarding a proposed security review and certification process for all voting systems; it also requires the Government Accountability Office (GAO) to	no provision	Sec. 10 requires an identical security review study as Sec. 3(a) of <b>S. 1986</b> , but also requires it to include a description of the voting system certification process required by §231 of HAVA; Sec. 10 also requires a similar report on operational and management systems as Sec. 3(a)	no provision	no provision	no provision

H.R. 2239/S. 1980	S. 1986	S. 2045	S. 2313	H.R. 4187	S. 2437	H.R. 4966
	issue a report to Congress (unless the EAC has already done so), within three months after enactment, on the operational and management systems that should be used to safeguard the security of voting systems, and a schedule for implementation.		of S. 1986, but requires that in addition the report examine such systems for federal elections generally and security standards for manufacturers, and that the report be done by the EAC.			
<b>Extension of Title I Payments</b>						
Sec. 2(a) and (b) would have extended the deadline for requesting payments under title I of HAVA to November 2003. Sec. 2(c) extends the authorization period for appropriations under title I to include FY2004 and would have	no provision	Sec. 3(a) and (b) extend the deadline for requesting title I payments to November 2, 2004. Sec. 3(c) extends the authorization period for appropriations under title I through FY2005 and extends the date on which unobligated and returned title I funds would be	Sec. 4(a) extends to August 1, 2004, the deadline for requesting an extension of the deadline for replacing punch card and lever machine voting systems.	no provision	no provision	no provision

<b>H.R. 2239/S. 1980</b>	<b>S. 1986</b>	<b>S. 2045</b>	<b>S. 2313</b>	<b>H.R. 4187</b>	<b>S. 2437</b>	<b>H.R. 4966</b>
extended the date on which unobligated and returned title I funds would be transferred to the EAC for use in requirements payments to January 1, 2004.		transferred to the EAC to January 1, 2005.				
<b>Repeal of EAC Contracting exemptions</b>						
Sec. 3 repeals §205(e) of HAVA, which provides the EAC with an exemption from a government contracting requirement.	no provision	Sec. 8 is identical to Sec. 3 of <b>H.R. 2239/S. 1980</b> .	Sec. 6 is identical to Sec. 3 of <b>H.R. 2239/S. 1980</b> .	no provision	no provision	no provision
<b>Effective Date</b>						
Sec. 8 stipulates that provisions in the bill will take effect as if they had been included in HAVA when it was enacted, except that the repeal of the contracting exemption will be	Sec. 4 is similar to Sec. 8 of <b>H.R. 2239/S. 1980</b> but does not include the contracting exemption.	Sec. 9 is similar to Sec. 8 of <b>H.R. 2239/S. 1980</b> , but also stipulates that the security requirements in Sec. 7 will apply to voting systems in use beginning November 2, 2004.	Sec. 11 is similar to Sec. 8 of <b>H.R. 2239/S. 1980</b> .	Sec. 3 is similar to Sec. 4 of <b>S. 1986</b> .	Sec. 2(b) is similar to Sec. 4 of <b>S. 1986</b> .	Sec. 5 stipulates that provisions in the bill will take effect with the November 2006 federal election except as otherwise specified.

<b>H.R. 2239/S. 1980</b>	<b>S. 1986</b>	<b>S. 2045</b>	<b>S. 2313</b>	<b>H.R. 4187</b>	<b>S. 2437</b>	<b>H.R. 4966</b>
effective upon enactment of the bill.						