WILL YOUR VOTE COUNT?: CAN THE CURRENT SOFTWARE WITHSTAND AND GUARANTEE THE CONSTITUATIONAL RIGHT TO VOTE?

Matthew Fisher*

Cite as: 8 J. HIGH TECH. L. 91 (2008)

Introduction

The right to vote is fundamental, receiving protection under the Fifteenth, Nineteenth, Twenty-fourth and Twenty-sixth Amendments to the United States Constitution.[1] Following the 2000 election, the United States of America witnessed the disruptive power of a faulty voting system, as the results of the presidential election were delayed five weeks due to Florida's inability to count votes.[2] In response to the 2000 election, Congress enacted the Help America Vote Act of 2002[3] (HAVA) as a vehicle of change to encourage the states to adopt more current voting technology, specifically, electronic voting machines that do not utilize punch cards or levers.[4] Protecting and guaranteeing the right to vote, a right fundamental to the operation of democracy, forms the basis for pushing the adoption of direct record electronic (DRE) voting machines in order to take advantage of the opportunities offered by the use of modern technology.[5] However, technology experts are concerned about the actual security provided by DRE machines,

* J.D. candidate 2008, Suffolk University Law School.

[1] *See* U.S. CONST. amends. XV, XIX, XXIV, XXVI; *see also* Yick Wo v. Hopkins, 118 U.S. 356, 370 (1886) (stating that the right to vote is an essential factor in ensuring protection of the rest of one's rights).

[2] *See* Bush v. Gore, 531 U.S. 98, 103-04 (2000) (stating that an estimated two percent of all ballots cast across the country cannot be registered and punch card voting machines do not meet the standards required in a national election); Juliet Eilperinand & Mike Allen, *Election Reform Gets Push From Bush, Congress*, WASH. POST, Jan. 25, 2001, at A1.

[3] Help America Vote Act of 2002, 42 U.S.C. § 15301 (2005).

[4] *See Id.* at § 15302.

[5] *See* Help America Vote Act of 2002, Pub. L. No. 107-252, 116 Stat. 1666 (2002) (stating in the preamble that the purpose of the law is to "establish minimum election administration standards for States and units of local government with responsibility for the administration of Federal elections").

especially the ability of the machines' software to withstand attacks.[6]

This Note will examine the forms of electronic voting that are available and assess the ability of each to protect the constitutional right to vote promised to every citizen of the United States of America that is eighteen years of age or older. It will illustrate the need to replace the existing system with a safe and secure form of electronic voting. It is imperative to meet the constitutional standards of security required in protecting the right to vote. Adequately protecting the right to vote will require active government involvement, continual testing of voting machines and security assurances for any form of electronic voting utilized.

Part I of this Note describes the attitude of the courts towards the use of technology when casting one's ballot and traces the development of voting technology. Part II describes the types of DRE systems available and the safety concerns connected to each particular form of electronic voting. Part III analyzes previously suggested remedial measures and proffers new ideas to protect against election fraud.

I. History of Voting Technology

A. History of Court Protection of the Right to Vote

The Supreme Court formally recognized the right to vote as being fundamental to the proper functioning of American democracy for the first time in 1886 in *Yick Wo v. Hopkins*.[7] At the same time, the Court allowed legislatures to impose justified limitations and requirements on voting.[8] In *United States v. Classic*,[9] the Court stated that "included within the right to choose, secured by the Constitution, is the right of qualified voters... to cast their ballots and have them counted."[10]

[6] *See generally* Tadayoshi Kohno, Adam Stubblefield, Aviel Rubin & Dan Wallach, *Analysis of an Electronic Voting System*, IEEE Symposium on Security and Privacy 2004 (2004) (on file with the author) [hereinafter *Hopkins Report*] (providing results of an analysis of the safety and security of a paperless electronic voting machine made by Diebold and vulnerabilities of the operating software to attack); *see also* Jon Stokes, *How to Steal an Election by Hacking the Vote*, ARS TECHNICA, Oct. 25, 2006, http://arstechnica.com/articles/culture/evoting.ars (detailing potential types of hacking attacks any voter, technician or other person accessing the DRE voting machine could carry out against it).

[7] 118 U.S. 356, 370 (1886) (finding that even though the right to vote is not specifically stated in the Constitution, its exercise preserves all other rights).

[8] *Id.* at 371.

[9] 313 U.S. 299 (1941) (holding that a person cannot be denied the right to vote and have that vote count in a federal election because of constitutional guarantees).

[10] *Id.* at 315.

The historical line of cases firmly entrenched the importance of the right to vote while indicating a judicial impatience with any practice that would impede its exercise. Although *Yick Wo* was decided in 1886, it was not until the Court agreed to hear the issue under dispute in *Baker v. Carr*[11] that voting issues received serious consideration before the Supreme Court.[12] In *Baker*, the Court found the Equal Protection Clause defeated a claim that a redistricting plan created a nonjusticiable political question beyond the power of the courts to decide.[13] The Court furthered its foray into voting rights analysis in *Wesberry v. Sanders,*[14] by holding that a person's vote cannot be reduced in efficacy and that all citizens are entitled to have their voice heard during an election.[15] In *Reynolds v. Sims*,[16] the Court stated that "the right of suffrage can be denied by a debasement or dilution of the weight of a citizen's vote just as effectively as by wholly prohibiting the free exercise of the franchise."[17] The Court completed the application of the one-person, one-vote doctrine by including local governments in *Avery v. Midland County*,[18] finding that the Fourteenth Amendment forbade any abridgment on the right to vote.[19]

Although previous cases had addressed the right to vote, *Bush v. Gore* represented the first time the Supreme Court focused on the machinery used to vote.[20] However, the *Bush* Court limited its decision to the specific facts of the case, declining the opportunity to voice a definitive opinion about the different available voting technologies.[21] The Court's language still sought to affirm that "the rudimentary requirements of equal treatment and fundamental fairness are satisfied."[22] The most

[11] 369 U.S. 186 (1962) (beginning judicial intervention into instances of district gerrymandering that served to undermine the impact of votes).

[12] Jessica Post, Note, *Uniform Voting Machines Protect the Principle of "One-Person, One Vote"*, 47 ARIZ. L. REV. 551, 558-59 (2005) (highlighting the Supreme Court's refusal to hear voting rights cases as well as describing cases in which the Court condoned infringements upon the right to vote).

[13] *Baker*, 369 U.S. at 234-37.

[14] 376 U.S. 1 (1964) (extending judicial oversight of improperly drawn voting districts to the state level by holding that state infringement of voting rights constituted a justiciable issue).

[15] *Id.* at 17-18.

[16] 377 U.S. 533 (1964) (another case considering the impact of a failure to reapportion districts on a person's right to vote).

[17] *Id.* at 555.

[18] 390 U.S. 474 (1968) (extending the implication of voting protections to all levels of government by finding that even in a local election a voter is entitled to be heard)

[19] *Id.* at 478-79.

[20] 531 U.S. 98 (2000).

[21] *Id.* at 109.

[22] *Id.*

important aspect of the *Bush* decision was the increased public awareness of potential complications associated with older forms of voting technology.

In 2003, *Weber v. Shelley*[23] became one of the first cases directly addressing the validity of DRE voting machines. The Ninth Circuit held that while the right to vote is fundamental, States can impose procedures to help ensure fairer elections.[24] Thus, even though a DRE machine may not produce a paper record, there is no valid vote denial claim if use of the machine is approved through a fair and indiscriminate review process.[25] The court explicitly recognized that although no voting system can completely eliminate the potential for fraud, some protections must be permitted to safeguard against it.[26]

A federal court most recently addressed the general issue of voting technology in *Stewart v. Blackwell*,[27] where petitioners challenged the continued use of punch card ballots.[28] The Sixth Circuit held that precedent requires implementation of adequate protections to ensure that all votes are counted equally.[29] If error-prone technology is used then unequal treatment can result, violating constitutional protections.[30] Technology that unfairly overvalues certain votes should not be used during the course of an election.[31] Even though DRE machines were specifically not at issue in *Blackwell*, it is possible to interpret the decision as requiring DRE machines to also ensure that sufficient protections are in place to guarantee the sanctity of every person's vote.

B. Development of Voting Technology

Originally votes were cast by choosing a straight party ballot printed by a particular party, eliminating the need to either select a candidate from a list or fill in a candidate's name.[32] In the 1880s, general fears of ballot inconsistencies and vote-buying led to enactment of reform

[23] 347 F.3d 1101 (9th Cir. 2003).
[24] *Id.* at 1105.
[25] *Id.* at 1106-7.
[26] *Id.* at 1106.
[27] 444 F.3d 843 (6th Cir. 2006).
[28] *Id.* at 846.
[29] *Id.* at 868-69.
[30] *Id.* at 869-70.
[31] *Id.* at 871-72.
[32] Eric A. Fischer, *Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues*, Congressional Research Service Report for Congress at 2 (Nov. 4, 2003), available at http:// www.epic.org/privacy/voting/crsreport.pdf (analyzing the history of different forms of voting technology used in the country, focusing upon the movement toward adoption of DRE technology). – copied how it was cited in an article on Westlaw – A.S.

legislation.[33] The main reform implemented the Australian ballot, a uniformly printed ballot where the act of voting occurs in secret and all candidates for all positions are listed.[34] While the Australian ballot solved one problem, it created another. Errors in counting hard copy versions of Australian ballots can still occur if the voter does not clearly mark the ballot or the human or machine counter incorrectly interprets the voter's intention.[35] Mechanical lever machines, first used in 1892, further protected ballots from tampering because a mechanical counter recorded each vote without producing a paper record that could be altered.[36] However, problems with machine levers arose if poll workers failed to properly adjust the lever, the machine did not record a vote, or someone tampered with the counters.[37]

As technology developed it became possible to use computers to aid in the vote counting process through the creation of a punch card that could be read by an optical scanner.[38] Due to the ease with which a vote can be made with a punch card and the continued state of anonymity, it quickly became the most popular form of voting.[39] A punch card also allows for quick tabulation of votes because the cards are fed into a machine that scans the holes in the ballot.[40] However, as illuminated by the 2000 presidential election,[41] problems occurred if the chad was not punched all of the way through.[42] Any type of voting error, whether by undervote (where all possible votes are not recorded) or by overvote (where multiple votes are marked on a question), will most likely result in the ballot not being counted and numerous voters being

[33] *Id*.

[34] *Id*.

[35] Daniel Tokaji, *The Paperless Chase: Electronic Voting and Democratic Values*, 73 FORDHAM L. REV. 1711, 1718-19 (2005).

[36] Fischer, *supra* note 32, at 3.

[37] Fischer, *supra* note 32, at 3.

[38] Fischer, *supra* note 32, at 3; *see also* Lillie Coney, *E-Voting: A Tale of Lost Votes*, 23 J. MARSHALL J. COMPUTER & INFO. L. 509, 510-11 (2005) (describing the quick adoption of punch card technology across the country and the manner in which an optical scanner read the markings on a ballot).

[39] *See* Tokaji, *supra* note 35, at 1719-20.

[40] Fischer, *supra* note 32, at 3.

[41] *See* Coney, *supra* note 38, at 511-12 (detailing complications with the chads known since the first use of punch card technology, which was well publicized in Florida during the 2000 election); David Von Drehle, et al., *In Florida, Drawing the Battle Lines; Big Guns Assembled as Recount Began*, WASH. POST, Jan. 29, 2001, at A1 (describing the problems experienced during the 2000 election in Florida and the preparation for the resulting legal battles).

[42] Tokaji, *supra* note 35, at 1720 (explaining that a chad is a perforated circle on a ballot that can be punched out, but can create complications if the stylus provided does not completely remove the chad or the ballot is misaligned, preventing the stylus from fully puncturing the chad).

disenfranchised.[43]

The newest voting technology utilizes direct recording electronic systems that are completely computerized.[44] These machines typically function much like an automatic teller machine ("ATM") at a bank, utilizing touch screen technology that creates an electronic record of each vote without a paper printout.[45] The DRE machine stores votes electronically, with the votes being submitted periodically throughout the day of the election or collected on data storage cards that can be removed as they are filled.[46]

Further taking advantage of technological developments, internet voting allows for online access of ballots any place that a voter can access the internet.[47] Internet voting can be divided into two main categories: remote, where the voter logs onto the appropriate website anywhere online access is available, or polling station, where a voting machine transmits votes over a closed network.[48] The two main criticisms associated with internet voting focus on network integrity and the difficulty in verifying the identity of remote voters.[49] A more complete description of electronic voting methods can be found in Part II of this Note.

C. The Help America Vote Act and Voting Technology

HAVA encourages states to utilize DRE voting machines through the provision of economic incentives.[50] The stated purpose of the law is to replace all punch card ballot systems across the United States of America with the creation of baseline standards for federal elections.[51] HAVA establishes the Election Assistance Commission (EAC), which is designated with the task of certifying and testing different voting system hardware and software.[52] HAVA also requires that testing and certification occur periodically to ensure that machines continue to

[43] Tokaji, *supra* note 36, at 1720.

[44] *See* Fischer, *supra* note 32, at 3.

[45] *See* Fischer, *supra* note 32, at 3-4.

[46] *See* Tokaji, *supra* note 35, at 1723-24 (describing the functioning of DRE voting machines).

[47] Bryan Mercurio, *Democracy in Decline: Can Internet Voting Save the Electoral Process?*, 22 J. MARSHALL J. COMPUTER & INFO. L. 409, 412-13 (2004) (describing the basic forms of internet voting currently available and the general manner in which they operate).

[48] *Id.* at 413-16.

[49] *Id.* at 438-47.

[50] Help America Vote Act, Pub. L. No. 107-252, 116 Stat. 1666, § 102 (2002) (codified as amended at 42 U.S.C. § 15302 (2007)).

[51] *Id.*

[52] *Id.* at § 201-2.

operate at acceptable levels and that an accurate tally of votes can occur.[53]

The EAC publishes guidelines for the testing and certification of voting machines in order to fulfill the requirements imposed by HAVA.[54] The manual states the certification procedures that software is supposed to follow prior to use in DRE machines during federal elections.[55] The testing program is designed to examine software prior to its receiving certification, representing a final hurdle needed before implementation.[56] A component of the process is a quality monitoring program, which attempts to follow the manufacturing process and ensure that DRE voting machines meet the accepted levels of quality.[57]

II. Current Problems with Electronic Voting

A. Events Demonstrating the Need to Transition

The 2000 presidential election exposed major flaws associated with the use of punch card ballots, especially the consequences of inaccurately recorded votes.[58] The prevalence of erratic voting machines undermined the ability to determine the actual intent of certain voters.[59] Following the election, Congress recognized the existence of a problem with the voting technology then being used.[60] As explained above, HAVA encourages States to update the types of machines used for elections, with special emphasis placed upon utilization of a system that satisfies minimum federal standards.[61] Congress delegated the

[53] *Id.* at § 231.

[54] *See Procedural Manual for the Election Assistance Commission's Voting System Testing and Certification Program*, 71 Fed. Reg. 76,281 (Dec. 20, 2006) [hereinafter *Testing and Certification Manual*] (describing the process by which the guidelines are published and the statutory mandate to create them).

[55] *Id.* at 76,284.

[56] *Id.*

[57] *Id.* at 76,299.

[58] *See* Drehle, *supra* note 41, at A1 (describing the fallout from the 2000 election and the fights between Albert Gore Jr., the Democratic candidate, and George W. Bush, the Republican candidate, over the efforts to count punch card ballots and determine the meaning behind hanging, dimpled, or other forms of chads).

[59] Paul Schwartz, *Voting Technology and Democracy*, 77 N.Y.U. L. REV. 625 (2002) (indicating the existence of a "voting-technology divide" that disproportionately affected different groups and possibly swayed the end result of the 2000 election because certain districts voted on more reliable machines).

[60] Audra Wassom, *The Help America Vote Act of 2002 and Selected Issues in Election Law Reform*, 29 T. MARSHALL L. REV. 357, 358-69 (2004) (explaining that Congress commenced consideration of HAVA following the 2000 election, finally enacting the legislation in 2002).

[61] *See* Post, *supra* note 12, at 555-56 (briefly summarizing the key provisions

power to determine acceptable voting machines to the EAC, which tests, certifies and decertifies machines as necessary.[62]

Following enactment of HAVA, States began developing plans to acquire new voting machines and phase them in for the 2004 presidential election.[63] Despite the concerns of electronic voting machine experts, the DRE machines performed adequately and did not experience the dire problems many feared.[64] The biggest problems arose in Ohio and Florida, with some machines displaying selections not made by voters and memory cards failing.[65] In response, an independent commission was formed following the 2004 election to study the complaints, with the commission suggesting that voting machines produce a paper trail in addition to conducting regular certification tests that ensure the accuracy of a DRE machine's vote count.[66] The commission concluded that the way to stop election fraud is to ensure such criminals are charged, brought to court and that these prosecutions are reported publicly.[67] In addition, they recommended poll watchers be present during elections.[68]

B. Problems Identified with DRE Machines

Numerous reports identify problems inherent in the various available DRE voting machines, including weak security measures and lack of a paper trail.[69] The California Task Force[70] focused upon the need for a

of HAVA and their intended impact).

[62] Fischer, *supra* note 32, at 7 (highlighting the EAC's role in implementing HAVA's requirements).

[63] *See* Tokaji, *supra* note 35, at 1737 (describing how major changes occurred in the types of voting machines used for the 2004 election, with about thirty percent of voters casting their vote on a DRE voting machine, but revealing that about three-quarters of voters across the country used the same form of voting machine as in 2000).

[64] *See* Tokaji, *supra* note 35, at 1740 (stating that no specific instances of fraud occurred as a result of a DRE machine being used, but admitting that some errors occurred).

[65] Stephanie Philips, *The Risks of Computerized Election Fraud: When Will Congress Rectify a 38-Year-Old Problem?*, 57 ALA. L. REV. 1123, 1147 (2006).

[66] *Id.* at 1147-48.

[67] *Id.* at 1149 (summarizing the independent commission's findings that emphasized the need to enforce penalties connected to election fraud).

[68] *Id.*

[69] *See* Tokaji, *supra* note 35, at 1735-36 (reciting the results produced by Professor Rubin et al. in the Hopkins Report that enumerated the security vulnerabilities of DRE voting machines); *see also* Fischer, *supra* note 32, at 8-10 (explaining the results of the California Task Force Report and the Hopkins Report, which both identified similar problems).

[70] A group organized by the California Secretary of State in 2003 to investigate the integrity and security of DRE voting machines in addition to developing

"voter-verified audit trail" in order to guarantee that a separate record of every vote is produced in the event a recount is needed.[71] The Hopkins Report studied the operating software of a Diebold machine and discovered it had poorly designed software that could be easily exploited and also found notes recorded by the coders that the software was not ready for broad use.[72] However, the studies are not without their flaws because the tests did not occur during an actual election.[73]

Additionally, problems with machines from Diebold and other manufacturers are repeatedly arising, raising more concerns over the viability of DRE voting machines.[74] Contentions over the safety of the machines resulted in California suing Diebold following the 2004 presidential election, alleging that Diebold overstated the integrity of the systems and lied about the certification procedures that the machines had undergone.[75] Problems concerning Diebold machines have not abated either, with Maryland experiencing complications with their DRE machines in 2004 and 2005.[76]

C. Nature of DRE Voting Machine Software Vulnerabilities

Concerns about DRE voting machines focus on weaknesses in the software source code that can expose the machines to manipulation and

recommendations for enhancements to the machines in order to guarantee the sanctity of votes cast. *See* Fischer, *supra* note 32, at 8.

[71] Fischer, *supra* note 32, at 8 (further suggesting that DRE machines not be used unless a paper trail is produced or recommending that machines be subject to random testing on Election Day until such a paper trail can be produced).

[72] *See* Hopkins Report, *supra* note 6, at 21 (expressing a fear that malicious codes could be introduced into the DRE machines that compromises their reliability unless a contemporaneous paper trail could be produced to allow for verification of the votes cast).

[73] *See* Tokaji, *supra* note 35, at 1778 (indicating that the Hopkins Report in particular did not test the DRE machines under the measures implemented during an actual election).

[74] *See* Tokaji, *supra* note 35, at 1779; *see also* Doris Long, *Electronic Voting Rights and the DMCA: Another Blast from the Digital Pirates or a Final Wake Up Call for Reform?*, 23 J. MARSHALL J. COMPUTER & INFO. L. 533, 540-43 (2005) (discussing the flaws found in the source code of the Diebold machines and the need to allow for independent testing of the code in order to protect against exploitation by hackers); *see also* Catherine Dolinski, *Voting Machine Malfunction Likely, Expert Testifies*, TAMPA TRIBUNE, Dec. 20, 2006, at 3 (relating expert testimony that without more extensive testing of software in DRE voting machines complications will probably continue).

[75] Philips, *supra* note 65, at 1147.

[76] Cameron Barr, *Md. Voting Machines had Faulty Part*, WASH. POST, Oct. 26, 2006, at B1 (describing problems in Maryland with screen freezing and random rebooting experienced while using Diebold machines and a general history of the difficult transition to DRE voting machines).

other security breaches.[77] The biggest complaint concerning the DRE machines centers upon the use of proprietary, not publicly disseminated, source code.[78] The integrity and quality of the code plays a large role in determining susceptibility to attack.[79] Critics argue that relying on proprietary code increases the likelihood that vulnerabilities will be present in the written code since only internal company developers test it.[80] With fewer opportunities to assess the code, the probability of a successful and undetected attempt to hack into the software increases.[81] Fears abound that the secrecy surrounding the code conceals the vote counting process from the public, further undermining faith in the accuracy of reported election results.[82]

The Digital Millennium Copyright Act ("DMCA") creates further problems because it allows DRE voting machine software developers to prevent unapproved people from examining their source code.[83] Any person wishing to examine proprietary source code copyrighted by another must acquire permission before obtaining the code and restrict research to activities that advance the general understanding of the encryption field.[84] An exception for security testing created by the

[77] *See* Philips, *supra* note 65, at 1143-50 (detailing coding problems found in DRE voting machines since 2000); *see* Tokaji, *supra* note 35, at 1775-77 (detailing coding problems found in DRE voting machines since 2000); *see* Fischer, *supra* note 32, at 12-15 (detailing coding problems found in DRE voting machines since 2000); *see generally* Andrew Massey, *"But We Have to Protect Our Source!": How Electronic Voting Companies' Proprietary Code Ruins Elections*, 27 HASTINGS COMM. & ENT. L.J. 233 (2004) (discussing the inherent problems associated with companies retaining proprietary control over the source code of the software that runs voting machines and calling for a move to open source code in order to allow the general public to test voting software for vulnerabilities).

[78] *See* Massey, *supra* note 77, at 241 (explaining that use of proprietary source code creates "security through obscurity" because developers hope that with the code being hidden from the public, the public will not be able to see the code and gain the ability to exploit latent weaknesses).

[79] Fischer, *supra* note 32, at 13 (the vulnerability of code to malicious coding increases with the complexity of the code because the number of hiding places increases as the code becomes more intricate).

[80] Massey, *supra* note 77, at 241.

[81] Fischer, *supra* note 32, at 13 ("Software code that is not well-designed from a security perspective is more likely than well-designed code to have points of attack and weaknesses that could be exploited, as well as places for malware to be hidden.").

[82] *See* Massey, *supra* note 77, at 243-44.

[83] *See* Long, *supra* note 74, at 535-38 (the DMCA provides protections to copyright holders that include creation of a safe harbor for internet service providers if they aid copyright holders in forcing an infringer to remove protected content from a website and establishing an abbreviated subpoena process for a copyright owner against an infringer).

[84] *See* Long, *supra* note 74, at 546-47 (further detailing that amateurs will not usually be awarded an exemption to study another's copyrighted code and the researcher can only reveal the results of the testing to the holder of the copyright).

DMCA appears to circumvent the above stated problems, but relief is elusive as the copyright owner still must consent to any such testing.[85]

Assaults on the physical DRE voting machine represent another potential avenue for compromising the security of the software operating the machines.[86] While some commentators recognize that destruction or vandalism of a machine is a possibility, such an attack is improbable.[87] A more likely form of the attack would be the use of a homemade smartcard, a card handed to each voter to activate the DRE machine.[88] Use of an unauthorized card could theoretically enable a voter to cast multiple votes, mimic an administrator, or alter the underlying code.[89]

A final vulnerability of the software system could occur during transmittal of the votes.[90] The theory at this stage envisions a hacker breaking into the internet connection used to send the data gathered throughout the day to a central database for counting.[91] Some machines use a direct modem connection in order to avoid use of a general internet connection, but the growing interrelatedness of various forms of communication exposes this route to attack as well.[92] As a result, the use of the internet to connect different polling stations is not a popular solution.[93]

III. Analysis

The criticism of DRE voting machines centers on the ability of the software running in the machines to guarantee the integrity of each vote cast.[94] Precedent shows that courts are not concerned with the form of

[85] *See* Long, *supra* note 74, at 547 (the language of the DMCA appears to prevent any outside researcher from testing the ability of protected source code to withstand attack).

[86] Tokaji, *supra* note 35, at 1776.

[87] Tokaji, *supra* note 35, at 1776.

[88] Tokaji, *supra* note 35, at 1776; *see also* Fischer, *supra* note 32, at 14-15.

[89] Tokaji, *supra* note 35, at 1776-77; *see also* Stokes, *supra* note 6, at 4.

[90] Fischer, *supra* note 32, at 14.

[91] Fischer, *supra* note 32, at 14.

[92] Fischer, *supra* note 32, at 14.

[93] Fischer, *supra* note 32, at 14.; *but see* Mercurio, *supra* note 47, at 411, 418-37 (advocating for the use of internet voting as a solution to increase voter turnout and decrease reliance on polling stations while proposing means of guaranteeing the integrity of a person's vote).

[94] The Hopkins Report studied the source code of a Diebold made DRE voting machine in order to assess manufacturer claims that the machines contained sufficient security features to thwart attempts to commit election fraud. Instead of a safe and secure system, the researchers discovered numerous flaws with programmers indicating in logs and comments areas of the code that needed to be improved before real world use of the software should have occurred. The researchers go so far as to say that "there appear[ed] to have been little quality control in the process," indicating that it would be easy for one person to influence

voting so long as the results are free of tampering.[95] Software concerns separate into two main categories: reliability and accuracy.[96]

A. Safety and Security of the Software

1. Open Source Code versus Proprietary Source Code

DRE voting machine manufacturers utilize proprietary code because this enables the manufacturers to take advantage of intellectual property protections, preventing substantive oversight.[97] By gaining protection for the software, most likely through copyright, the manufacturer of the DRE machine determines who can legally access and test the software.[98] Permitting a private company to exercise complete control over voting software enables the same private actor to remove transparency from elections.[99] The DMCA, enacted to update copyright laws for digital media, could potentially result in the copyright holder of voting software preventing any distribution of information about the copyrighted material.[100] The control granted by the DMCA also permits a software owner to limit security testing of the software to owners or operators, precluding the ability of outsiders, who may have more experience or time, from gauging the ability of voting software to protect the information generated during an election.[101]

an election through hacking. *See* Hopkins Report, *supra* note 6, at 21.

[95] *See Stewart*, 444 F. 3d at 870-71 (criticizing the use of different technologies that remove the equal opportunity to cast a vote and have it recorded, sustaining the implication that if the technology could be guaranteed to accurately record votes it would not matter what kind was used).

[96] *See* Tokaji, *supra* note 35, at 1734-37 (stating that studies distrust the ability of technology to adequately safeguard votes because of an inability to check the actual operation of the software or its precision in tallying the votes cast during an election).

[97] Massey, *supra* note 77, at 239-40 (describing the fact that software developers can obtain intellectual property protection solely for proprietary code because the source code is hidden from public view, thus enabling treatment of the source code as a trade secret).

[98] *See* Long, *supra* note 74, at 545-46 (discussing the impact of the DMCA on restricting access to copyrighted material and the right held by the copyright holder to be the only one who can decide when to expose their product to outside examination).

[99] *See* Long, *supra* note 74, at 546-47 (describing potential arguments for protection by changing the facts of an instance where students at Swarthmore College obtained proprietary code owned by Diebold and posted it on the internet).

[100] *See* Long, *supra* note 74, at 546-47.

[101] *See* Long, *supra* note 74, at 547 (specifically stating amateur testers would most likely be excluded by the narrowing restrictive language used in the DMCA while also explaining this exception places even more restrictions on outside testers than the encryption exemption, which allows any authorized person to examine the source code of a protected piece of software).

In hiding the source code from public view, it becomes impossible to conduct clear and transparent elections.[102] Proprietary code gives rise to new dangers by prohibiting public understanding of the operational procedures and risks associated with electronic voting.[103] The provisions of HAVA attempted to address concerns associated with DRE voting machine software through a mandate that voters have the opportunity to review and change votes in order to ensure the accurate recordation of voter intentions.[104]

However, without understanding the actual operation of the software, these protective steps instituted by law will prove ineffective.[105] Switching to open source code seems appealing because it opens the software up to public to viewing and testing.[106] Open source code based software is not usually copyrighted, enabling any user to experiment

[102] *See* Massey, *supra* note 77, at 241-42 (stating that protection of the public interest relies upon government operating in a "transparent and accountable" manner, where all citizens can verify that they have actual input and their rights are being safeguarded).

[103] *See* Massey, *supra* note 77, at 242-44 (voters are used to knowing how an election operates and expect an opportunity to confirm reported results if necessary).

[104] HAVA directly addresses this issue in Section 301 of the act, which provides the following:

> "SEC. 301. VOTING SYSTEMS STANDARDS. (a) REQUIREMENTS.—Each voting system used in an election for Federal office shall meet the following requirements: (1) In general. (A) Except as provided in subparagraph (B), the voting system (including any lever voting system, optical scanning voting system, or direct recording electronic system) shall— (i) 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; (ii) provide the voter with the opportunity (in a private and independent manner) to change the ballot or correct any error before the ballot is cast and counted (including the opportunity to correct the error through the issuance of a replacement ballot if the voter was otherwise unable to change the ballot or correct any error); and (iii) if the voter selects votes for more than one candidate for a single office— (I) notify the voter that the voter has selected more than one candidate for a single office on the ballot; (II) notify the voter before the ballot is cast and counted of the effect of casting multiple votes for the office; and (III) provide the voter with the opportunity to correct the ballot before the ballot is cast and counted."

Help America Vote Act of 2002, Pub. L. No. 107-252, 116 Stat. 1666 (2002) (codified as 42 U.S.C. § 15481 (Supp. 2002).

[105] *See* Massey, *supra* note 77, at 245 (stating that without the ability to conduct public testing of software code the public will not be able to trust the software because too many potential avenues for attack exist for hackers to access and corrupt the software); *see also* Wassom, *supra* note 60, at 384 (describing suspected tampering with DRE voting machines in Texas where voters claimed their screen selections were not accurately recorded and officials had no means of verifying the operation of the machines).

[106] *See* Massey, *supra* note 77, at 248 (claiming that the use of open source code would solve transparency and accountability problems because any person would be able to verify the safety of the software).

with the code in order to streamline the code writing and improve operation.[107] Despite the perceived benefits of utilizing open source code, the increased opportunity to exploit vulnerabilities naturally follows as a consequence of revealing the inner workings of a program to public consumption.[108] No consensus exists whether open source code produces more secure software because the more complicated source code becomes the more likely it is to contain flaws, regardless of the manner in which it is produced.[109]

The EAC attempts to achieve a middle ground with testing regulations that sustain the copyright protection enjoyed by DRE voting machine manufacturers under the DMCA.[110] The quality of the testing is uncertain, and there are not enough reviewers to thoroughly examine the submitted source code and certify that the software can meet the demands of an election.[111]

Although reservations exist about mandating the use of open source code, changes need to be made because elections involve exercising the

[107] *See* Massey, *supra* note 77, at 240 (discussing the benefits associated with open source code, specifically the intended lack of copyright protections over the original source code by the program's creator and revealing that while open source code can still qualify for copyright protection, it is designed to keep the compiled software open for public inspection, keeping its component parts freely viewable).

[108] *See* Fischer, *supra* note 32, at 26 (arguing that use of open source code instead of proprietary code exposes potential flaws to easier discovery and that maintaining use of protected code limits the number of people authorized to examine the software, thereby making it harder for people to take advantage of any problems).

[109] *See* Fischer, *supra* note 32, at 26; *see also* Ben Chelf, *Insecurity in Open Source*, BUSINESS WEEK ONLINE, Oct. 6, 2006, http://www.businessweek.com/technology/content/oct2006/tc20061006_394140.htm (offering the author's personal experience from analyzing both open source code and proprietary source code for bugs that errors occur with equal incidence, but then stating that use of proprietary code for mission critical applications is typically better given the extensive testing used and adherence to industry specific standards that open source coders are not compelled to follow).

[110] *See generally* Testing and Certification Manual, *supra* note 54, at 76,281 (creating the basic requirements to obtain certification of voting system software, requiring submission to an identified testing center, documentation of the manufacturer's procedures used to write the source code, and notification that the manufacturer can verify the contents of the code); *see also* Long, *supra* note 74, at 545-47 (discussing the protections over copyrighted works granted by the DMCA, and speculating that the statute could be used to stop unauthorized users from both testing and producing any information garnered about the software running inside voting machines).

[111] U.S. Gen. Accounting Office, *Federal Efforts to Improve Security and Reliability of Electronic Voting Systems are Under Way, but Key Activities Need to be Completed*, GAO-05-956, at 9 (September 2005) [hereinafter GAO Report], *available at* http://www.gao.gov/new.items/d05956.pdf (the EAC is still trying to develop clear guidelines for the testing and accreditation process, revealing the slow implementation of HAVA, and lack of clarity about federal standards).

right to vote, which must be free of taint.[112] The EAC took a step in the right direction with promulgation of its testing procedures.[113] Yet it is clear from the results of studies such as the Hopkins Report that the current testing scheme fails to discover vulnerabilities in the source code.[114] Relaxation of the protections enjoyed by DRE voting machine manufacturers under the DMCA through involvement of a larger community of testers provides a viable alternative.[115] Centering between the propriety and open source camps will meet the interests of both the DRE voting machine manufacturers, who want legal protections over their products, and the general public, who have an interest in voting in the safest way possible, while working to strengthen voting software to repulse attacks.

2. Susceptibility of Software to Outside Attack

The fear of an outside attack on a DRE voting machine occupies much of the public alarm over the use of electronic voting.[116] The possibilities for an attack on the software fit into three main categories, physical, code based, and result alteration.[117] The following analysis will consider attacks based on hacking the physical voting machine, remote access to the voting machine system or stored data, and communication breaches.

Physical hacking of the voting machine can occur through the use of

[112] *See* Long, *supra* note 74, at 548-49 (stating political speech enjoys protection under the First Amendment and identifying information concerning the operation of a DRE voting machine as involving political speech).

[113] *See* Testing and Certification Manual, *supra* note 55, at 76,290-91 (identifying the elements of the test plan and the necessity for the DRE voting machine manufacturer to submit the software for approval and testing by an authorized laboratory).

[114] *See generally* Hopkins Report, *supra* note 6 (detailing the bleak results obtained by the study group of source code from a Diebold election machine leaked onto the internet).

[115] Supporters of compelling the use of open source code believe that opening the testing process up to all people with software coding knowledge will produce optimal source code because the large volume of testers will be able to discover a large portion of the bugs in the software. *See* Massey, *supra* note 77, at 255-56. This takes a rosy view of both the ability and honesty of the general public in that if a person discovers a hard to find fatal flaw they will disclose the knowledge to the development community or the appropriate governmental authority that could take steps to prevent election fraud.

[116] *See* Fischer, *supra* note 32, at 12-16 (discussing the various vulnerabilities of DRE voting machines including the source code, unsecured connections to other computers, auditing transparency, and overall security policies).

[117] Tokaji, *supra* note 35, at 1775-77 (identifying types of attacks on DRE voting machines as consisting of the use of malicious code, attacks on the actual physical machine, result tampering, or other methods).

homemade activation cards or insertion of any other outside device.[118] Attacks occurring while a voter is in the polling booth would be easy to accomplish because of the standard of anonymity associated with voting.[119] Using a homemade smartcard presents an attractive hacking method of a voting machine because the ballot files are not encrypted.[120] Furthermore, if an attacker has any technical knowledge of the machines, the attacker could easily replicate a smartcard.[121] A hacker could also access the memory cards used and substitute their own or use the entry point to insert some form of malicious code.[122] Any violation of a DRE voting machine's physical defenses is cause for concern because it removes any assurances that one's vote remains one's own.[123]

The problem of preventing a physical attack appears easily correctable through institution of basic security measures at polling stations.[124] Possible measures could include a larger, more visible security personnel presence at election sites, and non-enclosed areas for housing the DRE voting machines when in use.[125] While these

[118] Hopkins Report, *supra* note 6, at 9-11 (describing the possible types of attacks that could occur with a homemade smartcard, including voting multiple times or accessing the administrator functions within the machine); Stokes, *supra* note 6 (describing the potential avenues of attack available to someone once they have violated the physical integrity of a voting machine, such as by accessing the Personal Computer Memory Card International Association (PCMCIA) slot where the data storage card is located).

[119] *See* Stokes, *supra* note 6 (recounting the experience of a Princeton University group that successfully accessed the PCMCIA slot on a DRE voting machine and uploaded a virus that could infect any other card inserted into the slot with vote stealing software in less time than it takes the typical person to vote).

[120] *See* Stokes, *supra* note 6; *see also* Hopkins Report, *supra* note 6.

[121] Hopkins Report, *supra* note 6, at 9 (detailing the ease with which any person could make their own smartcard due to the absence of cryptography in the voting machines and the widespread availability of tools to program and manufacture smartcards).

[122] Stokes, *supra* note 6.

[123] *See* Stokes, *supra* note 6. (discussing the fact that some states put security tape or tabs on the access slots, disqualifying a machine where visible tampering occurred and the possibility that a virus introduced into the machine can be transmitted to other machines if the infected card is placed into another one).

[124] *See* Fischer, *supra* note 32, at 16-17 (describing one element of defense plan as protection, which includes the presence of physical security to prevent unauthorized people form accessing voting machines in a manner that could compromise their integrity).

[125] While this may appear to be a violation of privacy usually seen in elections, it is well established that states can take measures necessary to guarantee the fairness and honesty of elections. *See Weber*, 347 F. 3d at 1105-06 (citing to a series of cases supporting the proposition that states are free to regulate the conduct of elections, which can extend to the actual voting process). If a DRE voting machine is kept in public view, then a potential attacker would not have the opportunity to access the PCMCIA slot or other data entry port to insert their own card, nor could a homemade smartcard easily be used since the person would be

suggestions diminish the privacy associated with voting, the reduced opportunity for tampering with the voting machines offsets the potential objections.[126] Physical attacks are a concern, but can be overcome through implementation of adequate security measures that still preserve the sanctity of the private ballot.[127]

The specter of a hacker breaking through the protections erected around election data and altering the stored information represents a potentially undetectable form of fraud that changes an election's ultimate result.[128] Election fraud of this type clearly violates the right to vote guaranteed to all citizens because one person gains control of the whole process.[129] Unless all votes cast on a particular DRE voting machine can be assured of receiving equal weight, the votes recorded on the machine will be suspect.[130]

The vulnerabilities of DRE voting machines to hacking during the course of an election can be directly related to the lack of encryption on the ballot information data files.[131] The easy access to data files represents a flaw in the software design process because adequate defense requirements are either not imposed or enforced.[132] Moreover,

under constant observation. The screen of the voting machine can also be shielded or produced in such a manner that only people standing in front of it can read the contents being displayed, thus preserving the essential need to keep votes anonymous.

[126] *See* GAO Report, *supra* note 111, at 40-42 (listing suggestions from the GAO concerning the implementation of increased security measures to ensure the validity of votes on DRE voting machines).

[127] GAO Report, *supra* note 111, at 40-42.

[128] Stokes, *supra* note 6 (identifying the various types of wholesale and retail election fraud that can occur, highlighting undetectable wholesale fraud as "the ultimate apocalyptic scenario"); *see also* Hopkins Report, *supra* note 6, at 11-17 (discussing the vulnerabilities of DRE voting machines to outside hacking and the ability for a hacker to either revise the recorded data or input completely new vote data in order to produce the result desired by the hacker).

[129] *See Stewart*, 444 F. 3d at 856-57 (recounting series of cases that identify the right to vote as essential to the proper functioning the government, with any violation of that right deserving severe punishment).

[130] *Id.* at 870 (stating that absent minimal guarantees against vote dilution those forms of voting technology implicated should not be used because it results in unfair and unequal votes).

[131] *See* Stokes, *supra* note 6 (explaining that the ballot definition files are not encrypted and it would be extremely easy for an attacker to insert a virus or manipulate the instructions coded into the file such that any vote cast will be altered to reflect the intentions of the attacker).

[132] Congress had the opportunity to address software integrity issues when enacting HAVA, but instead only focused on some of the widely reported problems. In HAVA, Congress required a paper trail and minimization of error rates in machine operation. Congress did recognize potential software issues through the creation of the EAC, which is supposed to test and certify machines, but undermined this development by failing to mandate that states only use EAC certified DRE voting machines. *See* Philips, *supra* note 65, at 1156-57.

concerns do not end with the election because a hacker can access unencrypted vote files during transmission to a central database or corrupt the files before transfer.[133] Again, the main part of the problem is the lack of encryption, which is a flaw within the software that can be remedied with application of appropriate standards and controls.[134]

The absence of protection is startling since the law manages to impose security requirements on banks for safeguarding financial information.[135] Election officials attempt to account for potential breaches of security by conducting logic and accuracy tests, but these tests fail to realistically simulate real-time election conditions and fall short of testing all of the active machines, among other problems.[136] Statutory or other regulatory schemes must look beyond the usually identified paper trail issue and ensure that the software controlling the full operation of the voting machines both during and after elections is secured.

A final consideration is the ability of software to permit safe transmission of voting data over the internet.[137] Security concerns with the internet focus on the ability of the software to keep intruders out.[138]

[133] *See* Stokes, *supra* note 6 (detailing the ability of a virus or other malicious program to spread should DRE voting machines be connected or the ability to corrupt the data card in one machine which will then corrupt any other machine it is placed into); *see also* Hopkins Report, *supra* note 6, at 15-16 (given the unencrypted nature of the data files stored within a DRE voting machine a hacker would be able to manipulate the files without detection, and if the votes are sent back to a central server the hacker could break into the connection, modifying the votes at this stage of the process too).

[134] The post-election checks established by HAVA focus not upon the ability to conduct an audit of the votes cast during the election, but focus upon the creation of a paper trail. *See* Wassom, *supra* note 60, at 381. However, this only addresses part of the problem because it ignores the fact that manipulation of the DRE voting machine's ability to properly count votes may already have occurred.

[135] The banking industry must assess foreseeable risks from both internal and external sources, look at the ability of existing policies to protect customer information, and other steps to control the potential risk of unauthorized use. To accomplish the goal of customer security four steps must be followed: design an information security program capable of controlling identified risks, train people to implement the plans, regularly test the security controls developed, and institute measures to properly delete information when it is appropriate to do so. 1-2A Computer Law § 2A.17 (MB) (2006)

[136] Stokes, *supra* note 6 (discussing the fact that a hacker could easily insert a virus or Trojan that only becomes active when the internal clock on a DRE voting machine reads the correct day of the election, taking advantage of the limited amount of time election workers have to test the voting machines and the fact that the logic and accuracy tests should only be one measure in a line of defenses designed to impede the ability of a hacker to easily penetrate the inner workings of the electoral system).

[137] Wassom, *supra* note 60, at 386 (identifying internet voting as a potential solution given its widespread use in modern society).

[138] Wassom, *supra* note 60, at 387 (expressing the concern that hackers would

However, a great number of people already trust the ability of internet based systems to maintain their financial privacy.[139] Additionally, regulations or other laws can be enacted to adopt minimum levels of security before a system will be certified.[140] At the same time, attacks on the internet server or software programs carry the same risks as attacks carried out on DRE voting machines located at polling stations.[141]

Solutions already exist to enhance the security of internet based software and "current security measures, such as Secure Sockets Layer, have [already] proven themselves to be safe means of transporting information over the Internet."[142] These assertions run counter to the common argument that internet connections will make elections less secure and that no voting machine should ever be connected to the internet.[143] An internet voting experiment conducted during the 2000 Democratic primary in Arizona showed no security breaches, suggesting that the internet could be a viable alternative with sufficient software security currently existing to guarantee the results.[144] The experiment proved that adoption of necessary safeguards and recognition of potential weaknesses goes a long way in protecting an electronically cast vote.

B. Recommendations for Change

It is clear that current law does not go far enough in addressing the security concerns associated with the use of DRE voting machines. No mandatory requirements exist that state minimum levels of quality for the operating software.[145] It is up to Congress, the States, or both to enact a regulatory scheme that ensures the software used in voting machines is vetted by experts and subject to comprehensive testing prior to being entrusted with the future of the United States of America.

The first step in the process involves the type of code used in the DRE voting machines. While arguments exist in favor of changing from proprietary to open source code,[146] a middle ground course is more

be able to access the voting system and alter votes or otherwise sabotage the election).

[139] *See* Mercurio, *supra* note 47, at 442.

[140] *See* Mercurio, *supra* note 47, at 443 (stating that software companies already include safeguards in products provided to help run elections as well as indicating a belief that in order for the convenience of voting to increase it is necessary to accept a corresponding reduction in security).

[141] *See* Mercurio, *supra* note 47, at 443-45.

[142] *See* Mercurio, *supra* note 47, at 444.

[143] *See* Tokaji, *supra* note 35, at 1792.

[144] Mercurio, *supra* note 47, at 414.

[145] 42 U.S.C. § 15371 (Supp. 2002).

[146] *See generally* Massey, *supra* note 77 (advocating for the switch to open source code because widening the investigatory process to the general public could

realistic. Manufacturers of DRE voting machines will not want to relinquish the protections currently afforded by copyright law.[147] The law should be amended to maintain copyright protection, while increasing the pool of qualified individuals who can obtain copies of the code in order to conduct security tests and modify the code as needed.[148]

Additionally, HAVA should be changed to enforce mandatory testing requirements on all voting machines and only permit use of EAC certified machines in federal elections.[149] Inclusion of liability for the DRE voting machine manufacturers for any inconsistencies related to foreseeable failures in the machines can provide further incentive to establish a thorough and careful production process.[150] Changes of this type could create a uniform standard for DRE voting machines and guarantee that the software running in them will secure vote data from outside manipulation.[151]

A final recommendation covers regular testing of the software for flaws. The law must require all DRE voting machines to be subject to at least annual testing under realistically simulated Election Day conditions.[152] It is impossible to determine the ability of a machine to

help improve the odds of discovering and correcting bugs in the software used to run DRE voting machines); *but cf.* Chelf, *supra* note 109 (arguing that proprietary source code is subject to more stringent requirements, resulting in better quality coding).

[147] *See* Massey, *supra* note 77 at 239-40 (explaining that current copyright law enables software producers to distribute compiled software which keeps the source code hidden and prevents others from using their property without permission).

[148] *See* Massey, *supra* note 77, at 240 (supporting use of open source code because it provides the benefit of allowing others to examine the code while preventing attackers from taking advantage of an unknown weakness in the software).

[149] *See* Wassom, *supra* note 60, at 379 (explaining that HAVA only includes recommended guidelines for the development of DRE voting machines).

[150] *See* Wassom, *supra* note 60, at 378 (criticizing HAVA for not including an individual right of action to enforce the provisions, providing inadequate resources for all levels of government to monitor compliance and failing to delegate administrative enforcement powers to the EAC).

[151] *See* Wassom, *supra* note 60, at 390-91 (recommending similar changes, but explicitly saying that a uniform ballot instead of DRE voting machine standards would remove local biases within ballots while improving the odds that voter confusion or incorrect voting do not occur).

[152] A complicated problem that would require technical studies of the procedures needed, but would need to include measures such as keeping the machines in operation for a period of time equal to that of a real election, a flow of voters comparable to a real election and other similar factors that serve the purpose of making the test run as authentic as possible. The GAO Report begins to go in the right direction by suggesting that all machines be subject to logic and accuracy testing. GAO Report, *supra* note 111, at 41. The GAO's recommendations fall short though because they do not explain how accurate tests can be conducted to mimic voting day conditions.

respond to certain conditions unless subjected to them.[153] Elections and the attendant results are particularly sensitive, so voting machines should be held to a higher standard.[154] Frequent testing will also serve to familiarize the volunteer poll workers with the machines, enabling them to more easily identify a compromised machine and enforce safety measures.[155]

IV. Conclusion

DRE voting machines as currently constituted contain many flaws. The software running inside the machines is flawed due to a lack of oversight in both creation and maintenance. With the implementation of proper regulations it will be possible to improve the software while significantly reducing the likelihood of outside attack.

While fears about technology exist, it is continually evolving; resisting adoption of its use in elections will only defer the problem. Implementation of appropriate testing and quality standards will ensure that the right to vote is not undermined while making it easier for all citizens to actively participate in the a basic part of the United States of America's democracy.

[153] *See* Stokes, *supra* note 6 (calling for testing of DRE voting machines at all stages of their development from manufacture to deployment as a potential means of discovering a hidden virus or malicious program before it causes real and irreparable harm).

[154] *See* Stewart, 444 F.3d at 860 (stating that the Equal Protection Clause in the Constitution requires everyone's vote to count equally and that methods of voting should not be used that cannot meet or exceed this standard).

[155] *See* GAO Report, *supra* note 111, at 41-42 (suggesting that election officials attend sufficient training to handle security and software complications that arise during the course of an election).