BRENNAN CENTER FOR JUSTICE

Committee on Oversight and Government Reform,
Subcommittee on Information Policy, Census, and National Archives

United States House of Representatives

Statement of

Lawrence D. Norden

Counsel, Brennan Center for Justice at NYU School of Law

May 7, 2007

The Brennan Center for Justice thanks the Subcommittee on Information Policy, Census and National Archives for holding this hearing. We appreciate the opportunity to share with you the results of our extensive studies to ensure that our nation's voting systems are more secure and reliable, as well as our thoughts regarding the challenges in developing more reliable accreditation and certification of voting systems. The Brennan Center for Justice is a nonpartisan think tank and advocacy organization that focuses on democracy and justice. We are deeply involved in efforts to ensure accurate and fair voting, voter registration, and campaign finance reform.

I. SUMMARY OF CHALLENGES TO ENSURE SECURE AND RELIABLE VOTING SYSTEMS

In less than five years, the vast majority of Americans have gone from using punch card and lever machines, to having their votes counted by electronic touch screens and optical scanners.[1] Unfortunately, as the Brennan Center and others have noted, this massive change took place without adequate development and implementation of procedures necessary to ensure that our new electronic voting systems were as secure and reliable as possible. In retrospect, the result of this failure was all too obvious: a crisis in public confidence in the voting systems most widely used across our nation and the certification and use of voting systems with serious security, accuracy and reliability flaws.

Fortunately, there is widespread agreement among experts about what must be done to make electronic voting more secure and reliable.

---

[1] Election Data Services, *2006 Voting Equipment Survey, available at* http://www.electiondataservices.com/EDSInc_VEStudy2006.pdf.

First, jurisdictions around the country must adopt basic security and reliability measures for machines already in use. Far too few of our states and counties take the steps necessary to greatly increase the security of our voting systems by making the least difficult malicious attacks against them much more difficult to execute successfully. Among the most important things jurisdictions can do are:

- **Conduct regular post-election audits comparing software independent voter verified records to electronic tallies**, to ensure that those tallies are accurate; and

- **Ban most wireless components on voting machines**, as they make voting systems far more vulnerable to many types of attacks.

Second, we must improve our process for federally certifying voting machines. The current process for certifying electronic voting machines is in transition, and there is reason to be optimistic that recent public exposure of some of the past problems will force important changes. At the same time, it is clear that for the last several years, the accreditation and certification process for voting machines has been flawed. To address the most serious of these flaws, the Brennan Center makes the following recommendations:

- **Ensure That Voting System Testing Laboratories Are and Appear to be Independent of Vendors.** Recent events have left many questioning the independence and competence of the laboratories that test and certify electronic voting systems. There are at least two things that can be done to begin to change this perception and create truly independent labs. First, we should end the process whereby the Voting System Testing Laboratories are chosen and directly paid by the vendors whose machines they evaluate. This creates an appearance of conflict of interest. Worse yet, it creates perverse incentives for the testing laboratories when testing vendors' machines. Second, the periodic evaluations of testing laboratories conducted by the National Voluntary Laboratory Accreditation Program ("NVLAP") should be made public promptly, regardless of whether the laboratory's accreditation is granted, denied or revoked.

- **Make the Voting Machine Certification Process More Transparent.** The recent CIBER debacle in New York has shown that testing laboratories sometimes fail to test even to current voting machine certification requirements. If the public is to regain its trust in this process, it is critical that the Election Assistance Commission ("EAC") publish: (1) all test plans submitted by the testing laboratories; (2) the vendor's Technical Data Packages, which the vendor submits to the EAC to provide the specifics of a voting system; as well as (3) the test report that a testing laboratory submits to the EAC after it has tested that voting system.[2]

[2] ACCURATE, *Public Comment on the Manual for Voting System Testing & Certification Program Submitted to the United States Election Assistance Commission* (Oct. 31, 2006), joined by the Brennan Center, *available at* http://accurate-voting.org/wp-content/uploads/2006/11/ACCURATE_VSTCP_comment.pdf (hereinafter "ACCURATE Comment on VSTCP").

- **Strengthen Voting Machine Certification Process Through Threat Analyses and Open-Ended Vulnerability Testing.** Currently, systems are certified by laboratories through "conformance" testing (i.e., the system is tested under normal conditions to ensure that it responds in a way prescribed by voting system guidelines). Computer scientists and security experts agree that good security testing must do more than this – specifically, it should attempt to ensure that a system will not fail when it is intentionally attacked or misused.[3] There are at least two important ways to address concerns around the limits of conformance testing. First, vendors should be required to demonstrate how their machines will defeat a standard set of threats developed by the National Institute of Standards and Technology ("NIST"). Second, independent security experts should be allowed to perform open-ended research for security and reliability vulnerabilities on voting systems.[4]

- **Use Information From Voters and Technical Experts Who Have Used the Voting Machines to Amend Voting System Standards, Where Necessary.** The EAC's Voting System Testing and Certification Program Manual now provides a formal (though severely limited) process by which election officials may report voting system anomalies. The Brennan Center joins other organizations in recommending that this reporting process be opened to include reporting from voters and technical experts who find anomalies.[5]

- **Adequately Fund the EAC and the Voting Machine Certification Process.** The EAC is the federal agency charged with overseeing many of the most important federal election administration tasks, including the accreditation of testing laboratories and certification of voting machines. However, its annual operating budget is $15 million and it employs fewer than 30 people.[6] If we are serious about reforming and improving the federal certification process, we must increase the EAC's budget and allow it to hire more staff.

---

[3] *See, e.g.*, Letter from Eugene Spafford, Chair, U.S. Public Policy Committee of the Association for Computing Machinery, to William Jeffrey, Director, National Institute of Standards Technology (Dec. 1, 2006) *available at* http://www.acm.org/usacm/PDF/USACMCommentsSTSPaper.pdf; *Voting Machines: Will the New Standards and Guidelines Help Prevent Future Problems?: Joint Hearing Before the H. Comm. on H. Admin. and the Comm. on Science*, 109th Cong. 136-148 (2006) (Responses by David Wagner, Professor of Computer Science, University of California-Berkeley to Post-Hearing Questions), *available at* http://www.votetrustusa.org/pdfs/qfr-house06.pdf.

[4] *See, e.g.*, U.S. Election Assistance Commission Public Meeting and Hearing, Pasadena, CA (July 28, 2005) (Testimony of David L. Dill, Professor of Computer Science, Stanford University and Founder of Verified Voting Foundation and VerifiedVoting.org) *available at* http://www.eac.gov/docs/Dill.pdf (hereinafter "Testimony of David Dill").

[5] ACCURATE Comment on VSTCP, *supra* note 2, at 8.

[6] U.S. Election Assistance Commission, *Fiscal Year 2006 Annual Report* 7 (2006) *available at* http://www.eac.gov/docs/EAC%20AR2006.pdf (hereinafter "EAC 2006 Annual Report"); Memorandum from Curtis Crider, Inspector General, U.S. Election Assistance Commission, to Thomas Wilkey, Executive Director, U.S. Election Assistance Commission (Oct. 2, 2006) *available at* http://www.eac.gov/docs/Memo%20on%20EAC%20noncomply.pdf (hereinafter "EAC Memo").

II. THE BRENNAN CENTER'S WORK ON VOTING SYSTEM SECURITY: HOW JURISDICTIONS CAN MAKE CURRENT VOTING SYSTEMS MORE SECURE AND RELIABLE

In 2005, in response to growing public concern over the security of new electronic voting systems, the Brennan Center assembled a task force (the "Security Task Force") of the nation's leading technologists, election experts, and security professionals to analyze the security and reliability of the nation's electronic voting machines.[7] The goal of the Security Task Force was simple: to quantify and prioritize the greatest threats to the integrity of our voting systems and to identify steps that we can take to minimize those threats.

Working with election officials and other experts for close to eighteen months, the Security Task Force analyzed the nation's major electronic voting systems, ultimately issuing *The Machinery of Democracy: Protecting Elections in an Electronic World* (the "Brennan Center Security Report") in June 2006. The conclusions of the Brennan Center Security Report are clear: (1) all of the nation's electronic voting systems have serious security and reliability vulnerabilities (including especially, vulnerabilities to the malicious or accidental insertion of corrupt software or bugs); (2) the most troubling vulnerabilities of each system can be significantly remedied; and (3) few jurisdictions have implemented any of the key security measures that could make the least difficult attacks against voting systems substantially more difficult to complete.[8]

Most importantly, the Task Force concluded:

- **Automatic audits, done randomly and transparently, are necessary if voter verified paper records are to enhance security.** The report called into doubt basic assumptions that many election officials and the public hold by finding that the use of voter-verified paper records without routinely comparing some portion of those paper records to the electronic tally – as is done in twenty-four states with voter-verified paper records – is of "questionable security value."

- **Voting machines with wireless components are particularly vulnerable to attack.** The report finds that machines with wireless components could be attacked by "virtually any member of the public with some knowledge of software and a simple device with wireless capabilities, such as a PDA."

- **The vast majority of states have not implemented election procedures or countermeasures to detect a software attack** even though the most troubling vulnerabilities of each system can be substantially remedied.

Among the countermeasures advocated by the Security Task Force are routine post-election audits comparing voter-verified paper records to the electronic record and bans on

[7] For a list of the members of the Security Task Force see Appendix A of this Statement.
[8] Lawrence Norden *et al.*, THE MACHINERY OF DEMOCRACY: PROTECTING ELECTIONS IN AN ELECTRONIC WORLD 3 (Brennan Center for Justice ed., 2006) *available at* http://brennancenter.org/stack_detail.asp?key=97&subkey=36343&init_key=105.

wireless components in voting machines. Currently only New York and Minnesota ban wireless components on all machines; California bans wireless components only on DRE machines. The Security Task Force also advocated the use of "parallel testing": Election Day testing of randomly selected voting machines under real world conditions. In jurisdictions with paperless electronic voting machines, meaningful audits of voter-verified paper records are not an option. Parallel testing allows these jurisdictions to detect the presence of malicious software in voting machines.

III. IMPROVING THE VOTING MACHINE ACCREDITATION AND CERTIFICATION PROCESS

The Voter Confidence and Increased Accessibility Act of 2007 (H.R. 811), introduced by Congressman Holt, adopts a number of key recommendations endorsed by the Task Force, including a requirement for mandatory, routine audits of voter-verified paper records for all federal races.[9] These are necessary steps to deter fraud and to catch programming errors, software bugs and other problems. However, audits will not, by themselves, improve the performance of our voting machines. Rather, they will allow us to learn, *after the polls have closed*, whether something has gone wrong.

For this reason, it is also important that we improve the federal process for certifying electronic voting machines so that we catch as many problems as possible *before* machines are certified and used in elections. That means ensuring that the laboratories certifying voting systems are truly independent, that the results of their tests are publicly available, and that the standards to which they test are as rigorous as possible.

A. Ensure That Voting System Testing Laboratories Are and Appear to be Independent of Vendors

If we are to have a certification process that works and inspires public confidence, it is critical that testing laboratories both are *and appear to be* truly independent of the voting system vendors whose machines they are testing. The procedures associated with laboratory accreditation that currently exist do not sufficiently address these concerns.

1. End the system that allows vendors to choose and directly pay voting system testing laboratories

Many election integrity advocates and security experts have criticized the current process by which vendors choose and pay the laboratories that evaluate their systems.[10] This process creates an appearance of conflict of interest for the testing labs. Worse still, it

[9] H.R. 811, 110th Cong. § 5 (2007).

[10] ACCURATE Comment on VSTCP, *supra* note 2; Testimony of David Dill, *supra* note 4; *Voting Machines: Will the New Standards and Guidelines Help Prevent Future Problems?: Joint Hearing Before the H. Comm. on H. Admin. and the Comm. on Science*, 109th Cong. 66-71 (2006) (Written Statement of David Wagner, Professor of Computer Science, University of California-Berkeley), *available at* http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1554&Itemid=26 (hereinafter "Testimony of David Wagner").

creates perverse incentives for the testing laboratories to certify machines to ensure that vendors choose them in the future. The testing laboratories themselves have done little to build public confidence in their independence from voting machine vendors. In a fairly well publicized written submission to the EAC, a testing laboratory recently stated that it "view[ed] the relationship between an independent testing laboratory and it's [sic] clients as similar to that between lawyer and client or between doctor and client."[11]

Given the many failures in the voting machine certification process in the last several years, it is critical that this system ends and that vendors have no role in choosing or directly paying the laboratories testing and certifying their machines. H.R. 811 would do this by establishing an escrow account with the EAC to which vendors would make payments for the costs of testing their machines. Vendors would have no role in choosing their testing labs; rather the EAC would choose the laboratories at random.[12]

2. Mandate publication of NVLAP Assessment Reports

The EAC's failure to timely publish a damning Assessment Report of CIBER, Inc. after is was completed in July 2006 provides a textbook case of how a lack of transparency can severely shake the faith of the public in the independence and competence of the laboratories testing and certifying our voting systems as secure and reliable. The report concluded, among other things, that:

> CIBER has not shown the resources to provide a reliable product. The current quality management plan requires more time to spend on managing the process than they appear to have available and it was clear during the assessment visit that they had not accepted that they have a responsibility to provide quality reports that show what was done in testing.[13]

As a result of the Assessment Report, the EAC determined it could not accredit CIBER under the interim accreditation process.[14] However, it did not publicize this decision, release the Assessment Report, or notify the State of New York, which was using CIBER to test its voting systems at the time. Only after the New York Times reported that CIBER had been barred from certifying election equipment and weeks of public pressure following that news article, did the EAC finally release the Assessment Report and other documents related to its decision.[15]

---

[11] U.S. Election Assistance Commission Public Meeting, Washington, D.C. (Oct. 26, 2006) (Written Statement of Frank Padilla, Test Supervisor, Wyle Laboratories, Inc.) *available at* http://www.eac.gov/docs/Voting%20Systems%20Briefing%20-%20Frank%20Padilla%2010-18-06%20Final.pdf.

[12] H.R. 811, *supra* note 9 at § 2.

[13] U.S. Election Assistance Commission, *Assessment Report: CIBER & Wyle* (conducted July 17-22, 2006) *available at* http://www.eac.gov/docs/Ciber%20&%20Wyle%20Assessment%20(July%202006).pdf.

[14] Christopher Drew, *Citing Problems, U.S. Bars Lab From Testing Electronic Voting*, N.Y. TIMES (Jan. 4, 2007) *available at* http://select.nytimes.com/search/restricted/article?res=F50811F63C540C778CDDA80894DF404482.

[15] These documents are available at: http://www.eac.gov/eac_vsc3_updates.htm.

Since the CIBER fiasco, NIST, through its National Voluntary Laboratory Accreditation Program ("NVLAP"), has taken over the process of assessing testing laboratories and making recommendations to the EAC regarding which testing laboratories should be accredited. To its credit, NVLAP has publicly released the Assessment Reports for the two laboratories it has reviewed and recommended for accreditation.[16]

However, there do not appear to be any written procedures requiring NVLAP to release such Assessment Reports. The public release of such reports, as well as reports connected to follow-up assessments, is critical to restoring the public's faith that the testing laboratories are competent and independent. Such publication should be required whether or not the laboratory receives or maintains its accreditation.

B. Make the Voting Machine Certification Process More Transparent

New York's recent experience with CIBER is also an excellent illustration of the importance of transparency in the voting machine certification process, and in particular the need to ensure that all test plans, Technical Data Packages and test reports are made public.

Concurrent with its hiring of CIBER to conduct its certification testing, New York also hired NYSTEC, a private, not-for-profit engineering company to conduct an independent review of CIBER's test plan. NYSTEC's review showed that the test plan lacked several security and functional testing requirements under state law and the federal Voluntary Voting System Guidelines of 2005 (to which CIBER had agreed to test). Among the items missing from the test plan were:

- A requirement that voting systems did not include any device potentially capable of externally transmitting or receiving data via the internet, radio waves or other wireless means;

- A requirement that voting system software not contain any viruses or other devices that could cause the system to cease functioning properly at a future time;

- A requirement for voting systems to provide a means by which the ballot definition code could be positively verified to ensure that it corresponded to the format of the ballot face and election configuration; and

- Test methods or procedures for the majority of the state's voting system requirements.[17]

These problems were only discovered because CIBER's test plans were subject to independent scrutiny. Short of mandating that jurisdictions hire independent reviewers for

[16] Information on the testing laboratories that NIST has reviewed is available at: http://vote.nist.gov/LabRec.htm.

[17] Howard Stanislevic, *Voting System Certification: Who's Minding the Store?*, VoteTrustUSA (Jan. 9, 2007) *available at* http://votetrustusa.org/index.php?option=com_content&task=view&id=2173&Itemid=113.

all certifications of voting machines, it is imperative that the EAC publish documents necessary for the public to ascertain the value of a testing laboratory's certification. This means not only publishing all testing laboratory test plans for a particular machine, but also the Technical Data Packages submitted by the vendor to the testing laboratory, and the laboratory's reports that assess the machines.

The EAC's Voting System Testing and Certification Program Manual now requires the publication of testing laboratory reports and test plans. It does not, however require the publication of all Technical Data Packages provided by the vendors for the reports; this omission will make it more difficult for the public and independent experts to judge the conclusions made in the laboratory reports.[18] This is a glaring gap in the EAC's reporting requirements and should be changed.

C. Strengthen Voting Machine Certification Process Through Threat Analyses and Open-Ended Vulnerability Testing

Currently, voting systems are certified by laboratories through "conformance" testing, which is meant to ensure that the voting system being tested will respond in a way proscribed by the federal voting system guidelines under normal conditions. Computer scientists and security experts agree that conformance testing is not sufficient to ensure that our systems are secure. As Professor David Wagner has pointed out in previous Congressional testimony, security evaluations should assume "an active, intelligent adversary; [conformance testing] concerns the presence of desired behavior, while security concerns the absence of undesired behavior."[19]

Princeton Professor Ed Felten's recent demonstration of a serious security flaw in a certified voting machine demonstrates the weakness of relying on conformance testing for security evaluations. Professor Felten and his co-authors showed that it was possible to insert malicious software onto a voting machine through the use of the machine's memory card slot. This flaw could allow a person with just a few seconds access to the memory card slot to "modify all of the records, audit logs, and counters kept by the voting machine."[20] While the flaw may have violated provisions of the voting system guidelines, these provisions were vague enough that it is easy to understand how lax testing could have missed it;[21] there was nothing in the guidelines that specifically prohibited a voting machine from being able to download code from a memory card or through a memory card slot.

---

[18] Aaron Burstein & Joseph Lorenzo Hall, *Unlike Ballots, EAC Shouldn't Be Secretive*, Roll Call (Jan. 22, 2007) *available at* http://www.rollcall.com/issues/52_66/guest/16640-1.html.

[19] Testimony of David Wagner, *supra* note 10.

[20] Ariel J. Feldman, J. Alex Halderman, & Edward W. Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine* 2 (Sept. 13, 2006) *available at* http://itpolicy.princeton.edu/voting/ts-paper.pdf.

[21] In his testimony Professor David Wagner notes that this security vulnerability may have violated Sections 6.4.2 and 6.2 of the FEC Standards. *Certification and Testing of Electronic Voting Systems: Field Hearing in New York, NY Before the Subcomm. on Info. Policy, Census, and Nat'l Archives of the H. Comm. on Oversight and Gov't Reform*, 110th Cong. 12 n.22 (2007) (Written Testimony of David Wagner, Associate Professor of Computer Science, University of California-Berkeley).

It is not reasonable to expect that we can develop a "check-list" that will imagine every possible flaw in a voting system. Clearly, however, finding such flaws before certifying machines is extremely important.

There are at least two important ways to address concerns around the limits of conformance testing. First, some form of threat analysis along the lines of that done by the Brennan Center Task Force on Voting System Security should be performed on all machines before they are certified. Specifically, vendors should be required to demonstrate how their machines will defeat a standard set of threats developed by NIST. Under no circumstances should software be the only defense against such attacks.[22]

Second, independent security experts should be allowed to perform open-ended research for security and reliability vulnerabilities on systems (these are often referred to as "red team exercises").[23] This is how many of the most serious vulnerabilities in electronic voting systems have been found.[24] Unfortunately, to this point, such flaws have been found outside the certification process, after machines were already certified and used in elections.

D. Use Information From Voters and Technical Experts Who Have Used the Voting Machines to Amend Voting System Standards, Where Necessary

Under the new Voting System Testing and Certification Program Manual, the EAC will accept reports from "[s]tate or local election officials who have experienced voting system anomalies in their jurisdiction."[25] This is an important step. Unfortunately, individual voters and technical experts performing usability, accessibility and security tests on voting machines appear to be excluded from filing such reports with the EAC.[26]

This is problematic for two reasons. First, the EAC has no method in place to protect the anonymity of election officials filing reports. Many election integrity and security experts have argued that an election official "might be reluctant to report an irregularity in a system he was responsible for administering," both because he may have

---

[22] *See* National Institute of Standards and Technology, *Requiring Software Independence in VVSG 2007: STS Recommendations for the TGDC* (draft, Nov. 2006) *available at* http://vote.nist.gov/DraftWhitePaperOnSIinVVSG2007-20061120.pdf (recommending that future systems be "software independent," meaning that an "undetected change in software cannot cause an undetectable change or outcome in an election.").

[23] Testimony of David Dill, *supra* note 4.

[24] *See, e.g.*, Michael A. Wertheimer, RABA Technologies LLC, *Trusted Agent Report: Diebold AccuVote-TS Voting System* (Jan. 20, 2004) *available at* http://www.raba.com/press/TA_Report_AccuVote.pdf; Harri Hursti, *Security Alert: July 4, 2005 – Critical Security Issues with Diebold Optical Scan Design* (on behalf of Black Box Voting, July 5, 2005) *available at* http://www.blackboxvoting.org/BBVreport.pdf; Feldman, Halderman, & Felten, *supra* note 20.

[25] U.S. Election Assistance Commission, *Testing and Certification Program Manual* section 8.7.2 (draft, Sept. 28, 2006) *available at* http://www.eac.gov/docs/Voting%20System%20Testing%20and%20Certification%20Program%20Manual%20FR%20DRAFT%20(Sept%2028).pdf.

[26] ACCURATE Comment on VSTCP, *supra* note 2, at 8.

also been responsible for purchasing that system and because he would probably need to continue to rely on technical assistance from the vendor.[27]

Second, voters and technical experts using these machines would be an excellent source of information about problems with these machines; in many instances, they will be in a far better position than election officials to know how the machines actually perform when used. We believe the reporting process should be opened to include them, and that the EAC should use credible reports from these sources to investigate potential problems with the machines, and mandate changes to the voting system guidelines or the machines themselves, when necessary.

E. Adequately Fund the EAC and Voting Machine Certification Process

The Help America Vote Act has placed the EAC in charge of many of the most important federal election administration tasks. Among other responsibilities – and aside from acting as the lead federal agency for accreditation of the Voting System Testing Laboratories and certification of voting systems – it is also charged with acting as a "clearinghouse of information on the experiences of State and local governments in implementing the guidelines and in operating voting systems in general," "conducting studies and carrying out other activities to promote the effective election administration of Federal elections," allocating election-related federal funding to the states, and carrying out administrative duties under the National Voter Registration Act of 1993 (the Motor Voter law), including developing and maintaining a mail voter registration application form for elections for federal office.[28]

Given its enormous responsibility, the EAC receives very little support. In 2006, it had an operating budget of just $15 million and employed less than 30 people.[29] Mandating the changes detailed in this testimony would be an important step in improving the accreditation and certification processes, but such mandates will have little effect if the EAC does not have the resources and staff to ensure such mandates are satisfied.

[27] *Id.*, at 9.
[28] 42 U.S.C. § 15322 (2003).
[29] EAC 2006 Annual Report, *supra* note 6; EAC Memo, *supra* note 6.

IV. CONCLUSION

The Brennan Center has found that the voting systems most commonly purchased today are vulnerable to attacks and errors that could change the outcome of statewide elections. This finding should surprise no one. A review of the history of both election fraud and voting systems literature in the United States shows that voting systems have always been vulnerable to attack. Indeed, it is impossible to imagine a voting system that could be impervious to attack.

But there are straightforward countermeasures that that will substantially reduce the most serious security risks presented by the three systems. The Brennan Center's recommendations point the way for jurisdictions with the political will to protect their voting systems from attack. None of the measures identified in the Brennan Center Security Report – auditing voter verified paper records, banning wireless components, using transparent and random selection processes for auditing, adopting effective policies for addressing evidence of fraud or error in vote totals, conducting parallel testing – are particularly difficult or expensive to implement.[30]

Reform and Support Process for Federally Certifying Machines. It is critical that we further develop clear standards and procedures that will mandate strict independence in the certification of machines, rigorous testing, and detailed reporting of tests and results. In addition, the entire process would benefit if the EAC used reports from voters and technical experts to amend voting systems standards and demand changes to voting systems where necessary. If we are serious about reforming the process for federally certifying machines, we must adequately fund the EAC.

[30] Even routine parallel testing and audits of voter-verified paper records – perhaps the most costly and time consuming countermeasures reviewed in the joint threat analysis – have been shown to be quite inexpensive. Jocelyn Whitney, Project Manager for parallel testing activities in the State of California, provided the Brennan Center with data showing that the total cost of parallel testing in California was approximately *12 cents per vote* cast on DREs. E-mail from Jocelyn Whitney (Feb. 25, 2006) (on file with the Brennan Center). Harvard L. Lomax, Registrar of Voters for Clark County, Nevada, estimates that a Task Force of auditors can review 60 votes on a voter verified paper trail in four hours. Assuming that auditors are paid $12 per hour and that each Task Force has two auditors, the cost of such audits should be little more than *3 cents per vote*, if 2% of all votes are audited. Telephone Interview with Harvard L. Lomax (Mar. 23, 2006). Each of these costs represents a tiny fraction of what jurisdictions already spend annually on elections. The Brennan Center's study of voting system costs shows that, for instance, most jurisdictions spend far more than this on printing ballots (as much as $0.92 per ballot), programming machines (frequently more than $0.30 per vote per election), or storing and transporting voting systems. Lawrence Norden *et al.*, THE MACHINERY OF DEMOCRACY: VOTING SYSTEM SECURITY, ACCESSIBILITY, USABILITY AND COST (Brennan Center for Justice ed., 2006) *available at* http://www.brennancenter.org/stack_detail.asp?key=97&subkey=38150&proj_key=76.

APPENDIX A: ABOUT THE TASK FORCE

In 2005, the Brennan Center convened a Task Force of internationally renowned government, academic, and private-sector scientists, voting machine experts and security professionals to conduct the nation's first systematic analysis of security vulnerabilities in the three most commonly purchased electronic voting systems. The Task Force spent more than a year conducting its analysis and drafting this report. During this time, the methodology, analysis, and text were extensively peer reviewed by the National Institute of Standards and Technology ("NIST").

The members of the Task Force are:

Chair
Lawrence D. Norden, Brennan Center for Justice

Principal Investigator
Eric L. Lazarus, DecisionSmith

Experts
Georgette Asherman, independent statistical consultant, founder of Direct Effects

Professor Matt Bishop, University of California at Davis

Lillie Coney, Electronic Privacy Information Center

Professor David Dill, Stanford University

Jeremy Epstein, PhD, Cyber Defense Agency LLC

Harri Hursti, independent consultant, former CEO of F-Secure PLC

Dr. David Jefferson, Lawrence Livermore National Laboratory and Chair of the California Secretary of State's Voting Systems Technology Assessment and Advisory Board

Professor Douglas W. Jones, University of Iowa

John Kelsey, PhD, NIST

Rene Peralta, PhD, NIST

Professor Ronald Rivest, MIT

Howard A. Schmidt, Former Chief Security Officer, Microsoft and eBay

Dr. Bruce Schneier, Counterpane Internet Security

Joshua Tauber, PhD, formerly of the Computer Science and Artificial Intelligence Laboratory at MIT

Professor David Wagner, University of California at Berkeley

Professor Dan Wallach, Rice University

Matthew Zimmerman, Electronic Frontier Foundation