BRENNAN CENTER FOR JUSTICE

Committee on House Administration, Subcommittee on Elections

United States House of Representatives

Statement of

Lawrence D. Norden

Counsel, Brennan Center for Justice at NYU School of Law

March 20, 2007

The Brennan Center for Justice thanks the Subcommittee on Elections 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. The Brennan Center for Justice is a nonpartisan think tank and advocacy organization that focuses on democracy and justice. We are deeply involved in the effort to ensure accurate and fair voting, voter registration and campaign finance reform.

I. THE BRENNAN CENTER'S WORK ON VOTING SYSTEM SECURITY AND POST-ELECTION AUDITS

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.[1] One of the key findings of the Security Task Force is by now widely accepted by computer scientists, many election officials, and much of the public: all of the major electronic voting systems in use in the United States have serious security and reliability vulnerabilities.

Many have advocated mandating voter-verified paper records as a solution to these vulnerabilities. In fact, voter-verified paper records by themselves will not address the security and reliability vulnerabilities the Brennan Center and many other groups have identified. To the contrary, as the Brennan Center Security Task Force noted in *The Machinery of Democracy: Protecting Elections in an Electronic World*,[2] voter-verified paper records, by themselves, are "of questionable security value." Paper records will not prevent programming errors, software bugs, or the insertion of corrupt software into voting systems.

---

[1] For a list of the members of the Security Task Force see Appendix A of this Statement.

[2] Lawrence Norden *et al.*, THE MACHINERY OF DEMOCRACY: PROTECTING ELECTIONS IN AN ELECTRONIC WORLD (Brennan Center for Justice ed., 2006) [hereinafter "Brennan Center Security Report"].

Voter-verified paper records will only have real security value if they are regularly used to check electronic tallies. It is for this reason that the Brennan Center urges Congress to adopt meaningful post-election audit legislation as soon as possible. Currently, only thirteen states require both voter-verified records and regular audits of those records.[3]

II. THE GOALS OF AN AUDIT AND HOW TO FULFILL THEM

How to use voter-verified paper records to check or "audit" the electronic records has, until recently, received very little attention, and even less systematic study. In *The Machinery of Democracy*, the Brennan Center made several audit recommendations, based in part on what we viewed as the best practices of the handful of states that already conduct regular audits.

Since the release of that report, the Brennan Center has teamed with the Samuelson Law, Technology & Public Policy Clinic at Boalt Hall School of Law (UC Berkeley), as well as several election officials and leading academics (collectively, the "Audit Group") to evaluate current audit laws and procedures and provide critical analysis to public officials as they begin to adopt audit schemes and procedures.

The Audit Group has identified several questions that legislators should ask before adopting an audit scheme and procedures. Among them are how, whether and to what extent the audits will:

1) increase public confidence in the results of an election;

2) deter fraud against the voting system;

3) detect large-scale, systemic errors;

4) provide feedback that will allow jurisdictions to improve elections and machines in future years;

5) confirm, to a high level of confidence, that a 100% manual recount would not change the outcome of the race.[4]

The Brennan Center has concluded that, among other things, an effective audit scheme that addresses these questions will do the following:

- **Use Transparent and Random Selection Processes for All Auditing Procedures.** Audits are much more likely to prevent fraud, and produce greater

[3] Those states are Alaska, Arizona, California, Colorado, Connecticut, Hawaii, Illinois, Minnesota, New Mexico, New York, Utah and Washington, West Virginia. *See* http://verifiedvoting.org/

[4] This is sometimes described as "confirm that the right candidate was declared the winner," though this is probably more than any statistical audit can guarantee.

voter confidence in the results, if the ballots, machines or precincts to be audited are chosen in a truly random and transparent manner.

- **Allow the Losing Candidate To Select Precinct(s) or Machine(s) To Be Audited.** In addition to conducting random audits, jurisdictions should allow a losing candidate to pick at least one precinct to be audited. This would serve two purposes: first, it would give greater assurance to the losing "side" that the losing candidate actually lost; second, it would make it much more likely that anomalous results suggesting a programming error or miscount were reviewed.

- **Place an Independent Person or Body in Charge of the Audits.** To increase public confidence that the audit can be trusted, it will be helpful to ensure that the person or persons supervising the audit are viewed as independent of the State's chief election officer, vendors who may have sold machines being audited, and any candidate running in an audited race.

- **Implement Effective Procedures for Addressing Evidence of Fraud or Error.** If audits are to have a real deterrent effect, jurisdictions must adopt clear procedures for dealing with audit discrepancies when they are found. Detection of fraud will not prevent attacks from succeeding without an appropriate response. Such procedures should also ensure that outcome-changing errors are not ignored.

- **Encourage Rigorous Chain of Custody Practices.** Audits of voter-verified paper records will serve to deter attacks and identify problems only if states have implemented solid chain of custody and physical security practices that will allow them to make an accurate comparison of paper and electronic records.

- **Audit a Minimum Percentage of Precincts or Machines for Each Election, Including At Least One Machine or Precinct for Each County in the State.** An audit that targets a fixed percentage (*e.g.* 3 percent) of machines or precincts to audit in each Congressional District is an efficient method for catching broad-based error or fraud. By auditing at least one machine or precinct in every county, jurisdictions will greatly increase the likelihood that they will find discrepancies caused by fraud or error at the county level.

- **Record and Publicly Release Numbers of Spoiled Ballots, Cancellations, Over-votes and Under-votes.** Audits that record the number of over-votes, under-votes, blank votes and spoiled ballots (including in the case of DREs, cancellations) could be extremely helpful in uncovering software attacks and software bugs and point to problems in ballot design and instructions.

- **Audit Entire System, Not Just the Machines.** History has shown that incorrect vote totals often result from mistakes when machine totals are aggregated at the tally server. Accordingly, good audit protocols will mandate that the entire system – from early and absentee ballots to aggregation at the tally server – be

audited for accuracy.

- **Increase Scrutiny in Close Elections.** Software bugs and/or tampering that affect the software of a small number of machines will generally not affect the outcome of federal elections. In extremely close races, of course, such problems can change the outcome of a race. In such cases, a 3 percent audit is unlikely to uncover a software bug, programming error or malicious attack that might alter the results of the race. Accordingly, the Brennan Center recommends that exceptionally close races receive heightened scrutiny.

III. BRENNAN CENTER AUDIT RECOMMENDATIONS IN DETAIL

There is a substantial likelihood that the audit procedures and other security countermeasures currently in place in most states would not detect a cleverly designed software attack program. Currently, only twelve of the states that require voter-verified paper records also mandate regular audits of those paper records to ensure that the electronic record is accurate.[5] Moreover, even those states that have mandated regular audits have not developed the best practices and protocols that are necessary to ensure their effectiveness in discovering attacks or failures in the voting systems.

Recommendation #1: Use Transparent and Random Selection Processes.

The development of transparently random selection procedures for all auditing procedures is key to audit effectiveness. This includes the selection of precincts and/or machines to be audited, as well as the assignment of auditors themselves. The use of a transparent and random selection process allows the public to know that the auditing method was fair and substantially likely to catch fraud or mistakes in the vote totals. In our interviews with election officials we found that, all too often, the process for picking machines and auditors was neither transparent nor random.

In a transparent random selection process:

- The whole process is publicly observable and, ideally, videotaped.

- The random selection is publicly verifiable, *i.e.*, anyone observing is able to verify that the sample was chosen randomly.

- The process is simple and practical within the context of current election practice so as to avoid imposing unnecessary burden on election officials.

The danger of non-transparent and non-random audits was made plain in Cuyahoga County, Ohio in 2004, when the Libertarian and Green Party Presidential candidates alleged problems with the general election results. In response to these allegations, the state mandated hand counts of ballots cast in 3 percent of the County's

[5] electionline.org, *Case Study: Auditing the Vote* (March 2007), *available at* http://www.electionline.org/Portals/1/Publications/EB17.pdf.

precincts, mandating a full recount if the 3 percent audit revealed discrepancies between the punch-card and electronic records. "Seeking to avoid a vast hand-count of thousands of punch-card ballots, election workers broke state law by pre-sorting the ballots to ensure they matched the final tally."[6] In other words, the audit was rigged to show no problems.[7]

The only way to ensure that we avoid the problems of Cuyahoga County in 2004 is to mandate that the selection of audited precincts be observable to the public and conducted in a truly random manner. The Voter Confidence and Increased Accessibility Act of 2007 (H.R. 811) sets important standards for transparency and randomness by requiring that audits shall be conducted "in a manner that allows for observation by the public,"[8] and that precincts be selected on an "entirely random basis using a uniform distribution in which all precincts" have an equal chance of being selected.[9]

Recommendation #2: Allow Losing Candidate To Select Precinct(s) To Be Audited

Several of the nation's leading experts on election security issues, including Professor Ronald Rivest of MIT, Professor Doug Jones of the University of Iowa and Professor Andrew Appel of Princeton University[10] have advocated allowing a losing candidate to pick additional precincts or machines to be audited. We think some variation of this suggestion is a good idea and endorse the recommendation.

This could be added to a statute as follows:

> At the request of any candidate who appears to have lost under the initial vote count, the chief auditor shall administer additional manual audits of at least [X] precincts or other audited units of the candidate's choosing, provided that the candidate reimburses the State for all expenses related to these requested manual audits, unless State law provides that the candidate need not make such reimbursement.

Such a procedure would serve two purposes: first, it would give greater assurance to the losing candidate and "side" that that the candidate actually lost; second, it would make it much more likely that anomalous results that could suggest a programming error or miscount would be reviewed.

---

[6] *Id.* at 5.
[7] *Id.*
[8] H.R. 811, 110th Cong. § 5 (2007).
[9] *Id.*
[10] *See e.g.* Andrew W. Appel, *Effective Audit Policy for Voter Verified Paper Ballots in New Jersey*, Center for Information Technology and Department of Computer Science, Princeton University (February 22, 2007), *available at* http://www.cs.princeton.edu/~appel/papers/.

Recommendation # 3: Place an Independent Person or Body In Charge of the Audits

Those in charge of the audit are likely to be responsible for selecting precincts or machines, calling for additional audits when anomalies or discrepancies are found, and ensuring that all information from the audit is made public. If the public is to be confident in the effectiveness of the audits, it is critical that these persons are seen as independent of both voting system vendors and candidates running in audited races.

The Count Every Vote Act of 2007 (H.R. 1381) and the Voter Confidence and Increased Accessibility Act accomplish this goal by establishing in each state an independent Chief Auditor and independent Audit Board, respectively.[11]

Recommendation #4: Implement Effective Procedures for Addressing Evidence of Fraud or Error

Audits are of questionable security value, and are far less likely to deter fraud, if jurisdictions do not have effective procedures for action where evidence of machine malfunction and/or fraud is uncovered. In the Brennan Center's extensive review of state election laws and practices, and in its interviews with election officials for *The Machinery of Democracy*, we did not find any jurisdiction with publicly detailed, adequate, and practical procedures for dealing with evidence of fraud or error discovered during an audit or recount.

The Voter Confidence and Increased Accessibility Act partially addresses these concerns by requiring a full publication of results of the audits, including all discrepancies discovered between the paper and electronic records.[12] We are hopeful that this increased transparency will make state and local election officials more willing to put in place effective procedures for investigating discrepancies when they occur.

We also recommend adding language *that requires* additional audits where discrepancies between the paper and electronic records in the audit are greater than the expected error rates for the relevant voting machines.

Recommendation #5: Encourage Solid Chain of Custody Practices

Audits of voter verified paper records will serve to deter attacks and identify problems only if states have implemented solid chain of custody and physical security practices. Missing or damaged paper or electronic records will make the reconciliation of audits all but impossible.

The Count Every Vote Act takes the important step of requiring the "appropriate State election official" to "develop and implement […] procedures to monitor and

[11] H.R. 1381, 110th Cong. § 102 (2007); H.R 811, 110th Cong. § 5 (2007).
[12] H.R. 811 at § 5.

document the chain of custody for election ballots, voter verified paper records, software, hardware and vote storage media before, during, and after an election for Federal office."[13]

We endorse this provision and recommend its inclusion in any voting security bill passed by this Congress.

Recommendation #6: Audit a Minimum Percentage of Precincts or Machines for Each Election

An audit that targets a relatively small but fixed percentage (*e.g.* 3 percent) of machines or precincts in each Congressional District is an efficient method for catching broad-based error or fraud. By auditing at least one machine or precinct in every county, jurisdictions will greatly increase the likelihood that they will find discrepancies caused by fraud or error at the county level (*i.e.*, in creating the ballot definition files or programming machines). They will also receive important feedback about the performance of specific machines throughout the state.

In many states, it will be far more efficient to audit by machine or ballot batches, rather than by precinct. Particularly in states that use touch-screen voting machines, jurisdictions will be able to achieve the same level of confidence in their results by auditing a smaller percentage of machines. The Voter Confidence and Increased Accessibility Act gives jurisdictions the flexibility of auditing by machine or vote batches, so long as the National Institute of Standards and Technology approves of their audit mechanism ahead of time.[14]

Recommendation # 7: Record and Publicly Release Numbers of Spoiled Ballots, Cancellations, Over-votes and Under-votes

Audits that record the number of over-votes, under-votes, blank votes and spoiled ballots (including in the case of DREs, cancellations) could be extremely helpful in uncovering software attacks or software bugs. This would be particularly true if such results were made public.

At least one study has purported to show that the majority of voters do not thoroughly check their voter verified paper records.[15] If a voter does not check her paper record, the paper record does not provide extra security for that voter. A vote could be misrecorded on both the paper and electronic record, and the voter (and election officials) would not realize votes were incorrectly recorded.

---

[13] H.R. 1381 at § 101(c).
[14] H.R. 811 at § 5.
[15] Ted Selker and Sharon Cohen, *An Active Approach to Voting Verification* (CalTech/MIT Voting Technology Project, VTP Working Paper #28, 2005) at 2, *available at* http://www.vote.caltech.edu/media/documents/wps/vtp_wp28.pdf.

However, if even a very small percentage of voters check their paper records thoroughly, an unusual number of cancellations on the paper trail will provide evidence that there was some problem in the way the paper record was recording votes.

There is a similar reason for counting over-votes and under-votes on precinct count optical scans. Many voters have benefited from the fact that precinct count optical scan machines have an over- and under-vote protection. If a voter skips a race, or votes for two candidates in a race, the scanner now informs the voter of the error, and allows her to change her ballot, so that her intention will be accurately recorded. In *The Machinery of Democracy*, the Brennan Center demonstrates that a state-wide shut-down of this protection (or a "bug" that accidentally shut it off) could result in the loss of tens of thousands of votes, mostly in low-income communities.[16] A review of the number of over and under-votes in an audit would provide evidence that something went wrong with this protection.

Moreover, this data will be extremely helpful to states, the Election Assistance Commission, academics and election integrity activists in assessing the effectiveness of ballot instruction and layout as well as the performance of specific machines. Post-election audits should be conducted not only to deter fraud and catch errors. They should also be used to provide important information on how well machines, ballots, and voters perform.

The Voter Confidence and Increased Accessibility Act requires the publication of the number of spoiled ballots, cancellations, over-votes and under-votes for each audited precinct or machine.[17]

Recommendation # 8: Audit Entire System, Not Just the Machines

History has shown that incorrect vote totals often result from accidents or tampering when machine totals are aggregated at the polling place or at the county tally server.[18] Accordingly, among other procedures, the Brennan Center has recommended legislative language that will:

- **Ensure That All Polling Places Compare Vote Tallies and Sign-in Sheets.** At close of the polls, vote tallies for each machine should be totaled and compared with number of persons that have signed the poll books. A comparison of these numbers should be made publicly available.

- **Ensure Individual Voting Machine and Precinct Totals Accurately Are Reflected in Tally Server Calculations.** A copy of totals for each machine should be posted at each polling place on Election Night and taken home by poll

[16] Brennan Center Security Report, *supra* note 1.
[17] H.R. 811 at § 5.
[18] *See, e.g.*, Anna M. Tinsley and Anthony Spangler, *Vote Spike Blamed on Program Snafu*, FORT WORTH STAR-TELEGRAM, Mar. 9, 2006 (noting that a programming error in the tally server software caused an extra 100,000 votes to be initially recorded in Tarrant County, Texas).

workers to check against what is posted publicly at election headquarters, on the web, in the papers, or elsewhere. This countermeasure allows poll workers and the public to ensure that corrupt or flawed software on a county's central tally-server does not incorrectly add up machine vote totals.

- **Mandate Daily Count of Early and Absentee Ballots.** The same audit procedures should apply to a daily count of early and absentee ballots, including, in the case of absentee ballots, the dates upon which the ballots were mailed and received.

We have not found these requirements in any bills that have been introduced in Congress this year and we strongly urge their inclusion in any voting system security bill that the House considers.

Recommendation #9: Increase Audit Scrutiny in Close Elections

For many races, a 3 percent audit will be more than sufficient to have confidence that a full recount would not result in a different outcome. However, in very close races, such an audit will not provide significant assurance that a software bug, programming error or malicious attack did not alter the results of an election.

This can be seen in the chart below, which looks at a typical Congressional District (the "Model Congressional District") of 400 precincts (for purposes of simplicity, it is assumed that all precincts are of roughly equal size). In this analysis, it is assumed that if more than 20% of the ballots in any single jurisdiction were corrupted, election officials and the public would detect the corruption without an audit (this is a common assumption in academic literature on this subject):

No. of Precincts in Congressional District	Margin of Victory	Confidence Level Attained By 3% Audit[19]
400	5%	80%
400	1.75%	43%
400	0.75%	22%

As the chart above shows, as the race gets closer, we have less confidence that the 3 percent audit will catch a corruption of the electronic record that could have altered the results of an election. The reason for this is simple: if a race is decided by a margin of greater than 5 percent, a software bug that actually changes the result of the election will probably have to affect a fairly large number of votes. A 3 percent audit has a relatively good chance of catching such a wide-spread error. By contrast, the outcome of an election that is decided by only 1 percent of the votes could be affected by a software bug that corrupts only a small number of votes. It is unlikely we will find these corrupted or misprogrammed machines if we audit only 3 percent of a district's precincts.

[19] In districts with less than 400 precincts, or with wide variation in number of votes per precinct, these confidence levels will be even lower.

If we increase the percentage of precincts or machines to be audited in close races, we can at least partially address this problem. The Voter Confidence and Increased Accessibility Act attempts to do this by adopting a "tiered" adjustable audit. The boxed numbers represent the confidence level achieved in the Model Congressional District by this bill's proposal.

No. of Precincts	Margin of Victory	Probability in a 2% Audit	Probability in a 3% Audit	Probability in a 5% Audit	Probability in a 10% Audit
400	0.75%	15%	22%	34%	57%
400	1.75%	31%	43%	61%	86%
400	5.00%	66%	80%	94%	99%

Under this "tiered" approach, jurisdictions will have greater confidence that result-changing errors were caught than they would get from a flat, 3 percent audit for all races.[20]

The approach adopted in the Voter Confidence and Increased Accessibility Act seeks to balance the need to increase scrutiny in close elections with the legitimate concern of election officials that they should not be overburdened by uncertain and administratively costly audits. This can be seen in the chart below, which shows the number of federal races in recent history with margins that would have triggered the tiered audits set forth in the Act. In short, the number is exceedingly small – in a typical federal general election, the vast majority of states would not be required to conduct even a single increased audit.

Year	Federal Races Requiring 3% Audit (decided by more than 2% margin)	Federal Races Requiring 5% Audit (decided by between 1% and 2% margin)	Federal Races Requiring 10% Audit (decided by between 0% and 1%).
2002	461	3	4
2004	510	5	5
2006	451	7	10

In 2002, 2004, and 2006, having a tiered audit procedure as proposed in the Voter Confidence and Increased Accessibility Act would have had a cost that was negligibly greater than a flat audit of 3 percent, since almost all of the races would have been

[20] As some commentators have noted, where Congressional Districts have less than 400 precincts, or precincts that vary substantially in size, the confidence levels listed in this chart will fall. Nevertheless, the basic concept remains the same: by increasing the audit percentage in close races, we gain greater confidence that result-changing errors will be caught. *See e.g.* Ronald Rivest, *On Auditing Elections When Precincts Have Different Sizes*, Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology (March 18, 2007), *available at* http://theory.csail.mit.edu/~rivest/Rivest-OnAuditingElectionsWhenPrecinctsHave-DifferentSizes.pdf, and Howard Stanislevic, *Random Auditing of E-Voting Systems: How Much is Enough*, available at http/www.votetrustusa.org/pdfs/VTTF /EVEPAuditing.pdf

audited at the 3 percent level anyway (the first tier). The extra cost of performing some audits in the second and third tier contributes about 1/30th of the total audit cost.[21] Although having a tiered approach adds some complexity to the process, it does not add significantly to the cost of doing the audits; yet it increases one's confidence that election results are correctly reported for all races—even close races.

Moreover, there is already significant precedent in state law for the percentages established by these tiers. Several states already require and successfully complete post-election audits of 3, 5 and 10 percent of precincts or machines.[22] It should be noted that *some of these audits include dozens of races and ballot questions, as opposed to the one, two or (at most) three federal races that each Congressional District will be mandated to audit under the Voter Confidence and Increased Accessibility Act.*

Finally, and importantly, the Voter Confidence and Increased Accessibility Act leaves room for states to develop their own audit schemes, so long as the schemes provide an equivalent minimum level of confidence as the tiered, precinct based approach. This is significant for two reasons. First, it should allow jurisdictions to audit by machine, ballot batches, or other audit units. In many cases, this will greatly reduce the administrative cost and burden of the audit requirements. For instance, in states where there are more voting machines than precincts, auditing by machine should allow jurisdictions to audit fewer total ballots.[23] Second, it gives jurisdictions great discretion to study and develop innovative auditing mechanisms that may be specifically appropriate for their states.

The Brennan Center recommends slight modifications to the alternate audit mechanism in the Voter Confidence and Increased Accessibility Act to ensure that these goals are met, and to provide states with guidance from the National Institute of Standards and Technology as they develop alternative audit mechanisms. Specifically, we would change the language to read as follows:

> Use of Alternate Mechanism – Notwithstanding subsection (a), a State may adopt and apply an alternative mechanism to determine the number of voter-verified paper ballots that will be subject to the hand counts required under this subtitle with respect to an election for Federal office, so long as the National Institute of Standards and Technology determines that the

[21] This calculation assumes that costs of increased audits increased linearly with audit percentage.
[22] For instance, of the twelve states that require voter-verified paper records and post-election audits, Hawaii mandates the post-election audits of 10 percent of all precincts, Illinois mandates audits of 5 percent of all precincts, Colorado and West Virginia mandate audits of 5 percent of machines, Alaska mandates audits of enough precincts to account for at least 5percent of all votes, and New York mandates audits of 3percent of all machines. Connecticut's Secretary of State recently introduced legislation that would require a post-election audit of 20 percent of its precincts. electiononline.org *supra* note 3, at 12-17.
[23] The confidence level in any audit fundamentally depends on the number of units audited; the greater the number of audit units (precincts, machines, etc.), the greater the confidence. If a jurisdiction can audit the same number of units with fewer ballots per unit, it will maintain statistical confidence in its audits while reducing its administrative burden.

alternative mechanism is as transparent as the procedure under subsection (a) and is consistent with the guidelines set forth in Section X.

Section X -- GUIDANCE ON BEST PRACTICES FOR ALTERNATIVE AUDIT MECHANISM. Not later than May 1, 2008, the National Institute for Standards and Technology shall establish guidance for States to establish alternative audit mechanisms. Such guidance shall be based upon scientifically reasonable assumptions for the purpose of creating an alternative audit mechanism that will

"(a) require the hand-count of at least 2% of all precincts (or other audited units) within each Congressional District, and ensure, with at least [90/95/99]% statistical confidence, for each federal election held in the State, that a 100% manual recount would not alter the outcome of the election; or

"(b) be at least as effective as section 322(a) in ensuring that for each federal election held in the state, a 100% manual recount would not alter the outcome of the election.

AUTHORIZATION OF APPROPRIATIONS – There are authorized to be appropriated to the National Institute of Standards and Technology $100,000 to establish the guidance required by this section.

In conclusion, many of the nation's leading election and security experts have reviewed the tiered audit scheme adopted by the Voter Confidence and Increased Accessibility Act and have concluded that it is a clear improvement over a flat percentage audit for all races. They have stated that it "reasonably balances a number of interests: confidence in election results, deterrence of electoral fraud, audit cost, innovation in new audit designs, and the burdens of administrability and frequency of increased percentage audits." A copy of their analysis is annexed to this statement as Appendix B.

IV. CONCLUSION

The nation's move to electronic voting has had many benefits, including increased accessibility for disabled voters and increased efficiency in election administration. Unfortunately, academic studies and Election Day problems over the last several years have shown that these new machines also came with a cost: new security and reliability problems, as well as increased public doubt about the accuracy and fairness of our elections.

This does not mean that the move toward electronic voting was a mistake. The mistake would be to fail to develop federal standards and procedures for these new machines. Most importantly, if we are serious about addressing the unique security and reliability vulnerabilities of these new machines, Congress must adopt solid post-election audit legislation as soon as possible.

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

Exhibit B: Memo on H.R. 811 Audit Mechanism

To: Congressman Rush Holt

From:* Lawrence Norden, Brennan Center for Justice at NYU School of Law

Aaron Burstein, Samuelson Law, Technology & Public Policy Clinic, UC Berkeley School of Law

Joseph Hall, School of Information, UC Berkeley

David L. Dill, Department of Computer Science, Stanford University

Candice Hoke, Director, Center for Election Integrity, Cleveland State University

Walter Mebane, Department of Government, Cornell University

Freddie Oakley, Yolo County, CA, Clerk-Recorder

Ronald L. Rivest, MIT EECS Department

David Wagner, Department of Electrical Engineering and Computer Sciences, UC Berkeley

Date:** 1 February 2007

Re: Thoughts on Mandatory Audits

We write to support your decision to adopt a "tiered" approach to auditing of voter verified paper records in the Voter Confidence and Increased Accessibility Act of 2007. Our understanding is that the language in the bill is as set forth in Appendix A.

This replaces earlier language that would have required all states to audit 2% of all precincts under all circumstances. We believe the new language will give jurisdictions more confidence that they will catch programming errors, software bugs or attacks against voting systems. This audit scheme also seems to allow jurisdictions to develop other, innovative audit procedures on their own and still receive federal funding for such audits, as long as they are at least as effective as what is otherwise required. Finally, this scheme minimizes potential burdens on election officials by requiring increased levels of audits *only when races are exceptionally close*. Below we explain the reasons behind our consensus.

---

* The authors' affiliations are provided for identification purposes only. The views expressed in this memorandum are the authors' personal views. The authors do not purport to represent the views of their respective institutions.

** Updated on March 19, 2007

Discovery of Systemic Error vs. Confidence Level and the Development of the Tiered Auditing Approach

Some of your colleagues may want to know what percentage of precincts must be audited in order to ensure that there is not an "unacceptable" level of error.

In truth, it may be that attempting to prevent an "unacceptable" level of error on electronic voting machines through audits is too administratively burdensome. This is particularly true if we assume that a certain number of votes (e.g., 10 % or 20%) can be miscounted in a single polling place without giving rise to an independent investigation, and that some errors will be "clumped" into a relatively small number of precincts, rather than spread evenly among them.

Thus, we might say that the miscounting of 1% of all votes in a federal race is "unacceptable." In an imagined typical congressional district, with 400 precincts of roughly equal size, we would need to audit more than 10% of all precincts to have at least 90% confidence that an audit would discover an error causing a miscounting of 1% or more of the votes.

Mandating a 10% audit for all races would be a high burden on many States. And in the vast majority of races, a shift of 1% of the votes would not alter the outcome of the race. For that reason, we might say that while less than ideal, we are willing to live with the risk that audits will not catch the 1% counting error in races where such an error is not going to change the outcome of the race.

But in races decided by less than 1% (in recent history, this has represented less than one percent of all federal elections), we might say we are *unwilling* to accept this risk.

Typical Congressional District

It is therefore worth considering how well the tiered approach will perform if we ask how likely audits in this scheme are to detect errors that would change the outcome of a specific race. The table below gives the probabilities of detecting discrepancies in 2, 3, 5 and 10% post-election audits in a typical congressional district with 400 precincts for races with margins ranging from 0.5% to 5.0% (Note: the highlighted numbers give confidence levels for audits conforming to the tiered approach of the Voter Confidence and Increased Accessibility Act of 2007.)[24]

No. of precincts	Margin of victory	Probability in a 2% audit	Probability in a 3% audit	Probability in a 5% audit	Probability in a 10% audit
400	0.50%	10%	14%	22%	41%
400	0.75%	15%	22%	34%	57%
400	1.00%	18%	27%	40%	66%
400	1.75%	31%	43%	61%	86%
400	2.00%	33%	46%	65%	89%
400	5.00%	66%	80%	94%	99.6%

As you can see from this chart, in cases of narrow margins, adopting the tiered approach could give the public and jurisdictions considerably greater confidence that result-

[24] These calculations assume that a vote shift of 20% or more within a single precinct will be detected.

changing errors were caught than would a fixed-percentage audit, without putting an unreasonable burden on the vast majority of districts.[25]

Minimizing the Burden on Election Officials

This tiered audit approach has the benefit of providing increased security in close elections without placing an undue burden on election officials. We can see this in the chart below, which shows the number of Congressional races in recent history with margins that would have triggered the tiered audits set forth in the Act. If your audit scheme were required in the last three federal elections, the number of expanded audits would have been exceedingly small.

Year	Federal Races Requiring 3% Audit (decided by more than 2% margin)	Federal Races Requiring 5% audit (decided by between 1% and 2% margin)	Federal Races Requiring 10% audit (decided by between 0% and 1%).
2002	461	3	4
2004	510	5	5
2006	451	7	10

Thus, we see that in 2002, 2004, and 2006, having a tiered audit procedure as proposed in the Holt bill would have a cost that is negligibly increased compared to a flat audit of 3%, since almost all of the races would be audited at the 3% level anyway (the first tier). The extra cost of performing some audits in the second and third tier contributes about 1/30th of the total audit cost.[26] Although having a tiered approach adds some complexity to the process, it does not add significantly to the cost of doing the audits; yet it greatly increases one's confidence that election results are correctly reported for all races—even close races.

The tiered audit scheme adopted by the Holt Bill reasonably balances a number of interests: confidence in election results, deterrence of electoral fraud, audit cost, innovation in new audit designs, and the burdens of administrability and frequency of increased percentage audits.

[25] As some commentators have noted, where Congressional Districts have less than 400 precincts, or precincts that vary substantially in size, the confidence levels listed in this chart will fall. Nevertheless, the basic concept remains the same: by increasing the audit percentage in close races, we gain greater confidence that result-changing errors will be caught. *See e.g.* Ronald Rivest, *On Auditing Elections When Precincts Have Different Sizes*, Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology (March 18, 2007), *available at* http://theory.csail.mit.edu/~rivest/Rivest-OnAuditingElectionsWhenPrecinctsHave-DifferentSizes.pdf, and Howard Stanislevic, *Random Auditing of E-Voting Systems: How Much is Enough*, available at http/www.votetrustusa.org/pdfs/VTTF /EVEPAuditing.pdf

[26] This calculation assumes that costs of increased audits increased linearly with audit percentage.

Appendix A

The text of the tiered audit used by the Voter Confidence and Increased Accessibility Act of 2007:

(a) IN GENERAL.—Except as provided in subsection (b), the number of voter-verified paper ballots which will be subject to a hand count administered by the Election Audit Board of a State under this subtitle with respect to an election shall be determined as follows:

(1) In the event that the unofficial count as described in section 323(a)(1) reveals that the margin of victory between the two candidates receiving the largest number of votes in the election is less than 1 percent of the total votes cast in that election, the hand counts of the voter-verified paper ballots shall occur in 10% of all precincts (or equivalent locations) in the Congressional district involved (in the case of an election for the House of Representatives) or the State (in the case of any other election for Federal office).

(2) In the event that the unofficial count as described in section 323(a)(1) reveals that the margin of victory between the two candidates receiving the largest number of votes in the election is greater than or equal to 1 percent but less than 2 percent of the total votes cast in that election, the hand counts of the voter-verified paper ballots shall occur in 5% of all precincts (or equivalent locations) in the Congressional district involved (in the case of an election for the House of Representatives) or the State (in the case of any other election for Federal office).

(3) In the event that the unofficial count as described in section 323(a)(1) reveals that the margin of victory between the two candidates receiving the largest number of votes in the election is equal to or greater than 2 percent of the total votes cast in that election, the hand counts of the voter-verified paper ballots shall occur in 3% of all precincts (or equivalent locations) in the Congressional district involved (in the case of an election for the House of Representatives) or the State (in the case of any other election for Federal office).

(b) USE OF ALTERNATIVE MECHANISM.—Notwithstanding subsection (a), a State may adopt and apply an alternative mechanism to determine the number of voter verified paper ballots which will be subject to the hand counts required under this subtitle with respect to an election, so long as the National Institute of Standards and Technology determines that the alternative mechanism will be at least as effective in ensuring the accuracy of the election results and as transparent as the procedure under subsection (a).