Statement
National Committee for Voting Integrity (NCVI)
Joint Hearing by the House Committees on
Science and Administration
Voting Machines: Will New Standards and Guidelines Help Prevent Future Problems?
July 19, 2006

> *"Elections require an end-to-end concern for a wide variety of integrity requirements, beginning with the registration process and ballot construction, and continuing through vote tabulation and reporting." – Peter Neumann*

Our thanks go to the Committees for holding this joint hearing, "Voting Machines: Will New Standards and Guidelines Help Prevent Future Problems?" We would like to offer a special thanks to Chairman Ehlers for his leadership on these important issues, which are challenging to our nation's public election's process.

General Comments

The Voluntary Voting System Guidelines (VVSG) is an improvement in some respects over the standards created by the Federal Election Commission process for 1990 and 2002: the increased attention to accessibility for voters with disabilities and language minorities is a step forward over previous voting technology standards. However, the document's treatment of security, transparency, and auditability reflects no improvement over previous standards. In fact some sections of the VVSG pose serious challenges to election integrity and voter privacy.

Current State of Voting System Certification

We are very troubled by the decision of the EAC to keep in place the existing voting technology certification process beyond the period designated by HAVA. On August 18, 2005, the EAC announced that the current voting technology certification process will be in place until the spring of 2007, with only one change: instead of the National Association of State Elections Directors (NASED) providing oversight of the three NASED approved laboratories the EAC will perform that function.

> "Provide for interim accreditation of National Association of State Election Directors (NASED) accredited Independent Test Authorities (ITA). The EAC will develop a process to temporarily accredit current NASED ITAs. This temporary EAC accreditation is needed to ensure that certified test laboratories are available in the near term. It has been determined that the EAC will not receive a recommended list of testing laboratories from the NIST National Voluntary Laboratory Accreditation Program (NVLAP) until the spring of 2007."[1]

[1] U.S. Election Assistance Commission, Staff Recommendation: EAC Voting System Certification & Laboratory Accreditation Programs Adopted August 23, 2005: EAC Public Meeting, Denver, CO, available at, http://www.eac.gov/VSCP_082305.htm

Allowing the current three certification laboratories to remain until the spring of 2007, as the only accredited laboratories that can certify voting systems intended for use in public elections, will not have a temporary effect. This decision will negatively affect those laboratories that have shown an interest in being accredited to certify voting technology. It may also diminish the intended results of the promulgation of new voting technology standards, and undermine public confidence in the accreditation and certification process. We strongly object to the continuation of the NASED ITA established voting technology laboratory accreditation and certification process because it allows failed voting technology to pass certification, is in violation of HAVA Section 231(b)(1), ignores the work already begun by NIST to replace the NASED ITA process, and hinders transparency.[2]

The widely reported failures of voting systems, which have passed NASED ITA certification, cannot be ignored. The failures are too numerous to summarize in this letter, but a few of the more notable ones are worth recounting:[3]

> Sarpy County Recount (Nebraska): As many as 10,000 phantom votes were added in 32 of 80 precincts when a machine error doubled the votes during counting. Source: Channel Six Omaha NE WOWT, available at http://www.wowt.com/news/headlines/1164496.html. (Nov. 5, 2004)
>
> Broward Vote-Counting Blunder (Florida): Vote tabulation software changes amendment results when the maximum capacity of 32,000 is reached, and the software begins to subtract votes. Source: Channel 4 WJXT Florida, available at http://www.news4jax.com/politics/3890292/detail.html. (Nov. 4, 2004)
>
> Carteret County (North Carolina): A voting machine loses more than 4,000 votes leaving three races including the Superintendent of Public Instruction and the state Agriculture Commissioner's race in doubt. Source: WRAL.com available at http://www.wral.com/news/3891488/detail.html. (Nov. 4, 2004)
>
> San Joaquin County (California): The Secretary of State's test of Diebold's TSx voting system recorded that almost 20 percent of the touchscreen machines crashed during the election simulation. Based on the voting systems performance California refused to certify the use of Diebold's TSX voting system in public elections. Source: Oakland Tribune available at http://www.votersunite.org/article.asp?id=5818 (Aug. 3, 2005)

HAVA Section 231(b)(1) states that "not later than 6 months after the Commission first adopts voluntary voting system guidelines under part 3 of subtitle A, the Director of NIST shall conduct an evaluation of independent, non-Federal laboratories and shall submit to the Commission a list of those laboratories the Director proposes to be accredited to carry out the

---

[2] Lillie Coney, Testimony, U.S. Election Assistance Commission, Denver, Colorado, August 23, 2005, available at http://www.epic.org/privacy/voting/eac-8_23.pdf

[3] National Committee for Voting Integrity, Election News, 2004, available at http://votingintegrity.org/archive/news/e-voting.html.

testing, certification, decertification, and recertification provided for under this section."[4] Further, the law requires the EAC Commissioners to vote to approve the list of accredited laboratories, once submitted by the Director of NIST, for the certification of voting technology used in public elections. The Commission is also directed by HAVA to publish an explanation for the accreditation of any laboratory not included on the list submitted by the Director of NIST.

NIST began work two years ago to produce a list of accredited laboratories for the certification of voting systems. On June 23, 2004, NIST announced in the Federal Register that it was establishing an accreditation program for laboratories that perform testing of voting systems, including hardware and software components. On August 17, 2004, NIST's National Voluntary Laboratory Accreditation Program (NVLAP) hosted a public workshop to exchange information among NVLAP laboratories interested in seeking accreditation for the testing of voting systems under HAVA. NIST has also published the National Voluntary Laboratory Accreditation Program's Voting System Testing Handbook 150-22. The handbook outlined the technical requirements and guidance for the accreditation of laboratories under the NVLAP Voting System Testing laboratory accreditation program. Finally, on June 17, 2005, NIST published a solicitation for applications and fees from those laboratories interested in being considered in the initial group of applicant laboratories. The notice stated that accreditation would begin on or about September 15, 2005.

In light of the work already done by NIST to provide for a new list of laboratories to be certified by the EAC to conduct certification of voting technology, why is the process being delayed until 2007? The consequences for this delay may be a reduction in the number of new qualified laboratories seeking work in this area, further erosion of public trust in the election system, and more failed voting technology being deployed by states.

Transparency

Transparency is a key component of a functioning, healthy democracy. Transparency or open government is any effort by agencies to impart information to the public on the work of the government. Open government can be accomplished in a number of ways, which may include: public meetings, public rulemaking notices, reasonable public comment periods, access to rulemaking proceedings, official reports, and open records laws. The application of technology intended to provide a government service should not be excluded from open government objectives. In addition to the methods described, the adoption of technology should include efforts to involve the participation of those members of the public with relevant skills and training.

The guidance to states on the administration of elections should include strong support of open government procedures that allow public access to the election administration process. Historically, the election administration community, voting rights community, media, and partisan efforts looked closely at how elections were managed. Today, that list of constituencies has grown to include technologists, election reform advocates, and concerned citizens.

[4] Help America Vote Act Law, Public Law 107-252, available at http://www.fec.gov/hava/law_ext.txt.

Transparency is not part of the current laboratory testing and certification process for voting technology. The NASED process did not and would not provide information on the testing process for any voting system.[5] Further, NASED would not answer specific questions regarding a voting technology manufacturer or a specific voting system.[6] In California, Diebold was found to have used uncertified software on voting systems operated during public elections.[7] When asked by California election officials about their certification of Diebold's AccuVote-TSx voting system, Wyle Laboratories refused to discuss the status of the testing.[8] It was reported that Wyle Laboratory told the state that the information was proprietary. These conditions should not be tolerated, especially in light of the need to provide proof to the American public that the promise of HAVA will be fulfilled.

Audit

In the final version of voting system guidelines, too little focus is placed on the importance of conducting audits of election results. Post-election evaluation of the results is fundamental to election integrity. For audits to be credible, the same vendor that supplied the voting system being audited should not perform the audit. It is important to know when election systems perform as expected, and when they do not. For this reason, independent, verifiable, and transparent audits of election results should be routine.[9] California, Colorado, Connecticut, Hawaii, Illinois, Minnesota, New Mexico, New York, North Carolina, Washington, and West Virginia all have laws addressing election audits.[10] For example, California's audit law requires a 1% manual recount of voted ballots.

Audits should include a representative hand count of ballots or ballot images; examining documentation of the chain of custody of all voting technology; and the chain of custody on all unmarked, and marked ballots. States are well within their prerogative to determine how the results of audits will be treated, however, they should be strongly encouraged to incorporate audits into every aspect of election administration, and make the results public. States should be encouraged to engage the technology community in the decision-making process to help meet the unique needs of state or local governments to routinely audit their elections.

Today it is not enough that vendors assure states that paperless voting systems record and retain accurate vote information, those systems must be proven to do so. The record of systems

---

[5] House Science Committee's Subcommittee on Environment, Technology, and Standards, Hearing: "Testing and Certification for Voting Equipment: How Can the Process be Improved?" 108th Congress Second Session, June 24, 2004

[6] *id*.

[7] Thomas Peele, "State allows unapproved machines for March election" Contra Costa Times, January16, 2004
Ian Hoffman, "E-voting software problems worsens," Alameda Times-Star, May 15, 2004.

[8] Elise Ackerman, "Vote-machine labs' oversight called lax" Costra Costa Times, May 31, 2004

[9] David Dill, Testimony, Election Assistance Commission, July 28, 2005

[10] Verified Voting, Manual Audit Requirements, August 20, 2005, available at http://verifiedvoting.org/article.php?id=5816

failures that resulted in lost votes cannot be ignored. Ballots lost from electronic voting systems used in North Carolina and Florida in 2004 attest to the need for more rigorous voting technology standards.[11] There is also a need to ensure routine access to ballot images for recount and election audit purposes. In 2004 the California Primary election resulted in a legal challenge, *Soubirous v. County of Riverside*, when a candidate lost an election contest by 45 votes. The candidate was denied access to the memory and audit logs of the Sequoia electronic voting machines purchased the Riverside County Board of Supervisors, which resulted in a court challenge.[12]

Security

Security can be defined as a series of tradeoffs.[13] For example, automobile manufacturers initially opposed interior airbags in cars because they were thought to be too costly. The government made the decision that their inclusion in cars would save lives and that the increased cost for the purchase of an automobile was worth the tradeoff.

The voter is the only person who should know how they voted. That person should not be able to prove to anyone how they voted, nor should a ballot be associated with that voter.[14] The votes cast by voters should be recorded and retained free from error or manipulation. The ballots and votes cast should be secured from tampering, damage, machine failure, or loss.

---

[11] Voters Unite, Report, Myth Breakers: Facts About Electronic Elections, available at http://www.votersunite.org/MB2.pdf
"Electronic Voting Machines Lose Ballots Carteret County, North Carolina. November, 2004. Unilect Patriot DRE A memory limitation on the DRE caused 4,438 votes to be permanently lost. Unilect claimed their paperless voting machines would store 10,500 votes, but they only store 3,005. After the first 3,005 voters, the machines accepted -- but did not store -- the ballots of 4,438 people in the 2004 Presidential election. Jack Gerbel, president and owner of Dublin-Calif.-based UniLect, told The Associated Press that there is no way to retrieve the missing data. Since the agriculture commissioner's race was decided by a 2,287-vote margin, there was no way to determine the winner. The State Board of Elections ordered a new election, but that decision is being challenged in the court.
Palm Beach County, Florida. November 2004. Sequoia DRE Battery failure causes DREs to lose about 37 votes. Nine voting machines ran out of battery power and nearly 40 votes may have been lost…. The nine machines at a Boynton Beach precinct weren't plugged in properly, and their batteries wore down around 9:30 a.m., said Marty Rogol spokesman for Palm Beach County Supervisor of Elections Theresa LePore. Poll clerk Joyce Gold said 37 votes appeared to be missing after she compared the computer records to the sign-in sheet. Elections officials won't know exactly how many votes were lost until after polls close."

[12] Soubirous v. County of Riverside, No. E036733, 2006 Cal. App. Unpsb. Lexis 1218 (Cal. App. Feb 8,2006) available at http://www.verifiedvoting.org/downloads/legal/california/soubirous-v-countyofriverside/

[13] Bruce Schneier, "Beyond Fear: Thinking Sensibly About Security in an Uncertain World" pg. 7.

[14] Coney, Hall, Vora, and Wagner, "Towards a Privacy Measurement Criterion for Voting Systems.

Voters should be able to cast votes and verify vote choices unassisted. Accuracy should be maintained and authenticated through a post-election audit process. State and local election contingency planning should detail what should be done in the event of a natural disaster or if a polling location unexpectedly becomes unavailable. Once an election has begun, contingency plans should cover what should take place to complete the election. For example, what should be done if a power outage occurs that exceed battery life of voting or ballot tabulation technology, voter turnout exceeds expectations, or unexpected shortages of Election Day poll workers occur, which threaten the conclusion of an election once begun.[15]

Reliability

Another technical threat to voting systems, which receives too little attention, is Electrostatic Disruption (ESD). This can be devastating to the operation of electrical equipment. Humidity and other conditions in which voting systems will operate can contribute to ESD. It is our view that more study should be done to better understand the threats that ESD poses to voting systems and develop means to mediate them. States should be directed to use a sliding scale for conditions, where machines will be used and ESD is a high probability.

Comments on Voluntary Voting System Guidelines

The Election Assistance Commission has demonstrated problems with version control of the final recommendations on voting system standards.[16] The problem has continued with the publication in the Federal Register the final guidance submitted to the EAC by the Technical Guideline Development Committee (TGDC) on their recommendations for voluntary voting system guidelines.[17] The TGDC recommendations sent to the EAC are available online.[18] The TGDC's online document representing their final recommendations to the EAC and the EAC's reprint of those recommendations in the Federal Register in April 2006 do not agree. Specifically the TGDC's final recommendations dated May 9, 2005 includes Sections 6.0.4.2.1.1.6 through 6.0.4.3.2.2, and the EAC document identified as the TGDC's recommendations document does not include these sections. The missing sections addressed the role of the NIST National Software Reference Library.

If this had been the only incident of version control problem it might not be noteworthy other than a correction be published in the Federal Register, but another earlier incident makes this appear to be a pattern of inefficient management of documents. For example in another

---

[15] Ace Project, Voting Operation: Contingency Plans, available at http://www.aceproject.org/main/english/po/poh01d.htm.

[16] National Committee for Voting Integrity, Letter (April 28, 2006)

[17] Election Assistance Commission, Technical Guidelines Development Committee's Final Recommendations on Voluntary Voting System Guidelines, Federal Register (April 12, 2006) available at http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/pdf/06-3101.pdf.

[18] TGDC final VVSG Document Delivered to the EAC May 6, 2006 available at http://vote.nist.gov/VVSGVol1&2.pdf.

incident the EAC voted on the final of the VVSG on December 13, 2005, the document was made public on January 12, 2006.[19] However, at some point between the public posting and mid-February the EAC final VVSG document was replaced by another version.[20]

Barring a thorough investigation of this issue—a solution may not be easy to achieve, however it is worth noting that the chief expertise of the National Institute of Standards and Technology (NIST) is the development of standards, and a key component of this work is version control. Therefore, we strongly recommend that the following action be taken, the correct TGDC VVSG document be printed in the Federal Register in its entirety, and that NIST be directed to manage version control for the EAC of all document development required under the Help America Vote Act (HAVA).

VVSG creates new threats to voting system security by recommending the use of telecommunication systems to transmit the election information over public telecommunication networks. Public telecommunication networks, especially the Internet, are insecure.[21] It is important to note that HAVA Section 245 directs that the EAC conduct a study and report on Electronic Voting and Electoral Process in federal elections.[22] The study, when completed, would assess the safe use of the Internet and other communication technology's use in voting.

It is our strong recommendation that future guidance issued by the agency to states direct them to prepare realistic contingency plans in the event of electronic voting system failures that jeopardize the completion of the election process.[23] Future Voluntary Voting System Guidelines should encourage state and local election administrators not to limit their thinking to what can be done, but to consider what can be done safely to establish reliable, secure, accessible, transparent, accurate, and auditable public elections.

In VVSG Volume 1, Section 7 Security, recommends the incorporation of wireless technology in voting systems. We strongly recommend that wireless technology not be allowed in voting systems. Although wireless technology is commonplace in remote control systems for televisions, DVDs, VHS, computer networks, and other consumer products that does not mean it should be trusted in voting systems. States considering wireless technology as an option should be strongly encouraged to enumerate the need for it, and evaluate the potential risks. Manufacturers of voting systems should not incorporate wireless technology as a standard offering in voting systems used in public elections because it poses serious security risks. The only way to be sure that the risk is not present is not to include the wireless capability. If states

---

[19] EAC, Final VVSG Document January 13, 2006 available at http://votingintegrity.org/pdf/vvsg_%20vol_I-1.pdf

[20] EAC, Current Final VVSG Document, July 14, 2006 available at http://www.eac.gov/VVSG%20Volume_I.pdf

[21] David Jefferson, Aviel D. Rubin, Barbara Simons, David Wagner, Report, "A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)", January 2004.

[22] Help America Vote Act of 2002 (HAVA), Public Law 107-252, October 29, 2002. SEC. 245. 42 USC 15385, available at http://www.fec.gov/hava/law_ext.txt.

[23] Ace Project, Report on Physical Security, available at http://www.aceproject.org/main/english/et/ete01a.htm.

insist on having wireless capability on voting systems, the next best security option is the ability to physically remove the device from voting systems before their use in public elections.

In closing, future recommendations to election administration should include a directive to test all ballot marking devices to be sure that they meet specifications of the precinct tabulating facility and central tabulating technology. The precinct tabulator and central tabulator technology should be calibrated to read reasonable marks, which should include a dark stroke crossing the voting target on its long dimension and half the width of the target should register as a vote. Finally, all ballot tabulators should be tested and/or calibrated to ignore erasures made by a new gum eraser of a thoroughly blackened pencil mark.

Guidance to states regarding the use of paperless direct recording electronic voting systems should include strong recommendations that at least one poll worker at each polling location should be trained to check the calibration of DRE voting machines and if necessary recalibrate them. Guidance to manufacturers should include criterion that these systems memory capacity is exceeded or a malfunction that threatens vote capture and retention is detected the voting system shall disallow the reinsertion of voter cards to disallow the appearance of continuing to record votes.

The United States is a society of equal rights. On Election Day, this nation must function as a society of equal rights, where a single vote is treated as important as the majority of votes cast.

Thank you,

MEMBERS

Peter G. Neumann, Chair * David Burnham * David Chaum * Cindy Cohn * Lillie Coney * David L. Dill * Joe Hall * David Jefferson * Jackie Kane * Douglas W. Jones * Stanley A. Klein * Vincent J. Lipsio * Justin Moore * Jamin Raskin * Marc Rotenberg * Avi Rubin * Bruce Schneier * Paul M. Schwartz * Sam Smith

NCVI Intern

Richard Rasmussen

[1] David Dill, Testimony, Election Assistance Commission, July 28, 2005
[1] Verified Voting, Manual Audit Requirements, August 20, 2005, available at http://verifiedvoting.org/article.php?id=5816
[1] Voters Unite, Report, Myth Breakers: Facts About Electronic Elections, available at http://www.votersunite.org/MB2.pdf
"Electronic Voting Machines Lose Ballots Carteret County, North Carolina. November, 2004. Unilect Patriot DRE A memory limitation on the DRE caused 4,438 votes to be permanently lost. Unilect claimed their paperless voting machines would store 10,500 votes, but they only store 3,005. After the first 3,005 voters, the machines accepted -- but did not store -- the ballots

of 4,438 people in the 2004 Presidential election. Jack Gerbel, president and owner of Dublin-Calif.-based UniLect, told The Associated Press that there is no way to retrieve the missing data. Since the agriculture commissioner's race was decided by a 2,287-vote margin, there was no way to determine the winner. The State Board of Elections ordered a new election, but that decision is being challenged in the court.

Palm Beach County, Florida. November 2004. Sequoia DRE Battery failure causes DREs to lose about 37 votes. Nine voting machines ran out of battery power and nearly 40 votes may have been lost…. The nine machines at a Boynton Beach precinct weren't plugged in properly, and their batteries wore down around 9:30 a.m., said Marty Rogol spokesman for Palm Beach County Supervisor of Elections Theresa LePore. Poll clerk Joyce Gold said 37 votes appeared to be missing after she compared the computer records to the sign-in sheet. Elections officials won't know exactly how many votes were lost until after polls close."

[1] Soubirous v. County of Riverside, No. E036733, 2006 Cal. App. Unpsb. Lexis 1218 (Cal. App. Feb 8,2006) available at http://www.verifiedvoting.org/downloads/legal/california/soubirous-v-countyofriverside/

[1] Bruce Schneier, "Beyond Fear: Thinking Sensibly About Security in an Uncertain World" pg. 7.

[1] Coney, Hall, Vora, and Wagner, "Towards a Privacy Measurement Criterion for Voting Systems.

[1] Ace Project, Voting Operation: Contingency Plans, available at http://www.aceproject.org/main/english/po/poh01d.htm.

[1] National Committee for Voting Integrity, Letter (April 28, 2006)

[1] Election Assistance Commission, Technical Guidelines Development Committee's Final Recommendations on Voluntary Voting System Guidelines, Federal Register (April 12, 2006) available at http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/pdf/06-3101.pdf.

[1] TGDC final VVSG Document Delivered to the EAC May 6, 2006 available at http://vote.nist.gov/VVSGVol1&2.pdf.

[1] EAC, Final VVSG Document January 13, 2006 available at http://votingintegrity.org/pdf/vvsg_%20vol_I-1.pdf

[1] EAC, Current Final VVSG Document, July 14, 2006 available at http://www.eac.gov/VVSG%20Volume_I.pdf

[1] David Jefferson, Aviel D. Rubin, Barbara Simons, David Wagner, Report, "A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)", January 2004.

[1] Help America Vote Act of 2002 (HAVA), Public Law 107-252, October 29, 2002. SEC. 245. 42 USC 15385, available at http://www.fec.gov/hava/law_ext.txt.

[1] Ace Project, Report on Physical Security, available at http://www.aceproject.org/main/english/et/ete01a.htm.

[1] U.S. Election Assistance Commission, Staff Recommendation: EAC Voting System Certification & Laboratory Accreditation Programs Adopted August 23, 2005: EAC Public Meeting, Denver, CO, available at, http://www.eac.gov/VSCP_082305.htm

[1] Lillie Coney, Testimony, U.S. Election Assistance Commission, Denver, Colorado, August 23, 2005, available at http://www.epic.org/privacy/voting/eac-8_23.pdf

[1] National Committee for Voting Integrity, Election News, 2004, available at http://votingintegrity.org/archive/news/e-voting.html.

[1] Help America Vote Act Law, Public Law 107-252, available at http://www.fec.gov/hava/law_ext.txt.
[1] House Science Committee's Subcommittee on Environment, Technology, and Standards, Hearing: "Testing and Certification for Voting Equipment: How Can the Process be Improved?" 108th Congress Second Session, June 24, 2004
[1] *id*.
[1]Thomas Peele, "State allows unapproved machines for March election" Contra Costa Times, January16, 2004
Ian Hoffman, "E-voting software problems worsens," Alameda Times-Star, May 15, 2004.
[1] Elise Ackerman, "Vote-machine labs' oversight called lax" Costra Costa Times, May 31, 2004