TEXAS CIVIL RIGHTS PROJECT

Michael Tigar Human Rights Center
1405 Montopolis Drive, Austin, Texas 78741-3438
(512) 474-5073 (phone) (512) 474-0726 (fax)

James C. Harrington
Director

July 24, 2009

Voluntary Voting System Guidelines Comments
U.S. Election Assistance Commission
1225 New York Avenue, NW, Suite 1100
Washington, DC 20005

Re: Voting System Guidelines Comments

To Whom This May Concern:

Enclosed please find my comments regarding the Voting System Guidelines (VVSG) version 1.1.

Thank you for your attention to this matter. If you have any questions, please do not hesitate to call my office.

Sincerely,

TEXAS CIVIL RIGHTS PROJECT

James C. Harrington
Director

TEXAS CIVIL RIGHTS PROJECT

Michael Tigar Human Rights Center
1405 Montopolis Drive, Austin, Texas 78741-3438
(512) 474-5073 (phone) (512) 474-0726 (fax)

James C. Harrington
Director

COMMENTS REGARDING VOTING SYSTEM GUIDELINES
By James C. Harrington, Director
July 24, 2009
UNITED STATES ELECTION ASSISTANCE COMMISSION

The Texas Civil Rights Project (TCRP) is representing the NAACP and voters in a litigation to prevent the Texas Secretary of State from using the Hart Intercivic eSlate, a direct recording electronic (DRE) voting machine that does not produce a voter-verified paper audit trail (VVPAT), for use in Travis County, Texas. I testified before the appropriate House committee in Texas in support of DREs producing VVPATs. The bill did not get out of the House committee, and the Senate did not consider the issue at all. The continued use of paperless DREs in Texas has seriously affected voters due to the inaccuracies and vulnerabilities of DREs. VVPATs are necessary in order to have sufficient record of cast votes in the event of DRE failure.

The use of DREs that do not produce a VVPAT in Texas, including the use of the Hart Intercivic eSlate in Travis County where our office is located, violates the fundamental right of citizens of the United States to vote in elections. DRE failure has occurred nationwide, and the probability of inaccurate vote counts is so great that thirty-three (33) states no longer permit use of DREs without an independently verifiable paper ballot. In fact, Texas is only one of eleven (11) states still using DRE as a sole source of counting votes in some of its counties. The continued use of DREs in Texas has resulted in a significant number of instances of DRE failure, some of the major ones of which include:

- In the 2004 presidential election, a DRE in Collin County froze. Attempts to retrieve the votes on the frozen DRE failed, despite assurances that such a thing could never happen due to multiple memories and fail safes.

- In March 2006, an undetected computer glitch caused an eSlate to inflate election results in Tarrant County, recording 100,000 votes that were never cast.

- In November of 2008, 160 complaints were filed in Bexar County due to DRE failure, including a DRE that crashed containing votes that could not be retrieved.

- In the 2008 presidential election, DREs flipped votes from Democratic to Republican selections, depriving voters from casting votes for their desired party in Collin, Dallas, El Paso, Galveston, Harris, Jefferson, and Palo Pinto Counties.

Experts agree that DREs are vulnerable to failure and viral attack, losing or misreporting votes in the process. Dan Wallach is a leading expert on DREs, an associate professor in the Department of Computer Science at Rice University in Houston, Texas, and has served as an

expert witness in seven different lawsuits concerning electronic voting, including a congressional election controversy in Sarasota, Florida. He is also the associate director of NSF's ACCURATE (A Center for Correct, Usable, Reliable, Auditable and Transparent Elections), a collaborative project involving six institutions investigating how security technologies may best be applied to electronic voting systems.

During the California Secretary of State's "Top to Bottom Review," Dr. Wallach was part of a team that considered the security of many electronic voting systems manufactured by several companies, as well as accessibility and documentation issues. The California study was the most comprehensive study of its kind ever performed, and the results are compelling. Significant security flaws were discovered for each of the reviewed DREs. Most notably, flaws were discovered that could be exploited to allow for "viral" attacks on an election. In such an attack, a single voter, in the privacy of a voting booth, would compromise the software of a single voting system. Subsequent to this, through the regular and proper actions of poll workers and election administrators, every voting system used in the county would become infected with the virus. Such a virus might, for example, flip votes in favor of a particular candidate or party. Alternately, such a virus might do nothing until a distinguished event occurs on the voting machine (e.g., a write-in vote for a specific fictional character), allowing the compromised machine to pass "logic and accuracy" or "parallel" testing without detection.

Companies that manufacture DREs claim to have security measures in place to prevent these sorts of attacks. Likewise, election administrators often claim that procedural measures offer mitigation against these threats. The vulnerabilities Mr. Wallach and his team discovered allow all of these measures and procedures to be easily bypassed, particularly in a state like Texas where electronic voting machines do not have VVPATs.

The Voluntary Voting System Guidelines (VVSG) set the quality standard for voting systems used in the United States. The Election Assistance Commission (EAC) has asked the National Institute of Standards and Technology (NIST) to change the current VVSG standard from "software independence" to that of "auditability." Software independence is defined as that "quality of a voting system of device such that a previously undetected change or fault in software cannot cause an undetectable change or error in election outcome." (VVSG-2007 Appendix A). To achieve software independence, it is necessary to design a voting system in such a way as to ensure that:

(a) the system will not mis-present choices to the voter, including an incorrect vote from the voter, and

(b) if there were a complete audit, any error made by the voting machine in receiving or processing the voter's votes would be detected.

Paperless DREs have no independent way to determine the validity of the vote count when errors occur. If a noticeable error in the vote count is discovered, paperless DREs have no way to determine the voters' intent. Thus, the accuracy of the total count is not reliable. Therefore, adhering to the software independence standard requires a verifiable paper record of each vote cast. Lowering the standard to auditability, as proposed by the ECA, may allow for the use of DREs that do not have a VVPAT or produce paper records. Thus, the EAC, in asking

NIST to lower the VVSG standard from software independence to auditability, sabotages both the security and accuracy of cast votes.

Cem Kaner, professor of software engineering at the Florida Institute of Technology, senior member of the Institute for Electrical and Electronics Engineers, and member of the Technical Guidelines Development Committee, commented on the auditability standard proposed by the EAC. Mr. Kaner notes that to achieve auditability, as the term is normally used, "a system need only provide features than enable or support the tasks of auditing. This in itself provides no assurance that a complete audit would expose all errors. Audits are rarely exhaustive and as we have so often seen in the financial systems, significant numbers of errors or irregular practices can escape the notice of a diligent auditor." Institute of Electrical and Electronics Engineers, Inc., *Brief Comments on EAC Research Areas for the TGDC VVSG Recommendations, available at* http://www.votetrustusa.org/pdfs/EAC/KanerCommentsFeb20 2009.pdf (Last visited July 23, 2009).

NIST has proposed to redefine the auditability standard: rather than employing its normal usage, auditability should be mean "the quality of a voting system or device such that any error in its recording of votes or vote totals, whether randomly occurring or maliciously induced, is detectable" for the VVSG. National Institute of Standards and Technology, *EAC Research areas for the TGDC VVSG Recommendations*, 3 (2009), available at http://www.eac.gov/program-areas/voting-systems/docs/nist-response.pdf/attachment_download/file. Mr. Kaner notes, and I agree, that it is "hazardous to redefine a widely-understood term with an unusual and precise technical definition, especially when many of the key stakeholders and decisionmakers will be unfamiliar with whatever regulation or standard redefines it." DREs that rely on internal software to record cast votes for an audit yet provide no voter-verified paper audit trail, such as those used in Texas, meet the normal usage of the term auditability. This is extremely problematic. The auditability standard may be misconstrued, allowing for the continued use of DREs producing no record capable of a meaningful audit. Given the number of instances of DRE failure experienced throughout Texas and other states that continue to use DREs without VVPATs, changing the software independence standard to NIST-auditability is risks jeopardizing the accuracy and security of the vote.

We are not in favor of replacing the software independence standard with the weaker standard of auditability. Software independence is key to a verifiable election and a functioning democracy. Sacrificing the security and reliability of voting systems by removing the software independence standard and replacing it with a vague notion of a standard will prevent citizens of the United States from exercising their fundamental right to vote. Interference with a right so firmly rooted in our democratic system is unjust and unnecessary.