Memorandum

To: Election Assistance Commission (EAC)
EAC Technical Guidelines Development Committee (TGDC)

From: Rebecca Mercuri <mercuri@acm.org> 215/327-7105, 609/587-1886
Senior Member, Institute of Electrical and Electronics Engineers (IEEE)
Fellow, Radcliffe Institute for Advanced Study, Harvard University

Date: December 20, 2004

Subject: Lack of Security Assurances and Auditability Requirements in the IEEE P1583 Draft 5.3.2 Voting System Standards

The draft version of the Voting System Standards (VSS) that you are receiving from the IEEE's P1583 working group is the product of three years of effort, the latter two years of which I have been an active participant. This draft, although considerably improved from the version that failed to gain approval when it was issued last year to the IEEE Standards Association, remains highly flawed. Many of its flaws are the result of legacy problems in the Federal Election Commission's 1990 and 2002 documents (on which the P1583 VSS was based and intended to replace), as well as an inability of the working group to gain consensus on numerous critical security assurances and auditability requirements for voting systems.

These flaws are salient because it has been the practice of the Independent Test Authorities (ITAs) to overlook inspection of aspects for which the standard remains silent. This has meant that certified voting systems have included such components as unsecured wireless transceivers or modems, outdated and insecure commercial-off-the-shelf (COTS) software, obsolete encryption schemes, and paper ballot printers that violate voter anonymity, without any cautionary advisories to purchasers. As well, the type of testing that is performed by the ITAs is far from comprehensive – for example, threshold flaws (like integer overflows) are not exercised, and security risks are not detailed. Since there is no process whereby the ITAs can recall or decertify products, some election systems have continued to be used long after (or in conditions where) they were proven to be unfit. A case where this was observed in 2004 occurred when certain optical ballot scanners started counting backwards when they reached 32K (a flaw that had been identified in 2002).

Although the current P1583 draft standard addresses some obvious security issues, it remains silent on a great number of topics, essentially providing a road-map to the back doors for the undetectable rigging of elections, especially by insiders (such as election officials, precinct workers, warehouse employees, vendor agents and repair personnel). Since elections are, by their very nature, adversarial processes where insiders have both opportunity and motive, these flaws, even if never exploited, give reason for considerable loss of confidence in election results by the general public. Such a collapse of confidence (even if not a computerized election) can have a destabilizing effect on a democratic government, as was recently seen in the Ukraine. This is especially true when the voting system provides no means whereby election results can be independently confirmed, as was the case in nearly 30% of counties in the United States in 2004.

In particular, the most severe flaws of the P1583 draft, in my opinion, are as follows:

COTS: Some industry members of the working group have claimed that vendors should be allowed to use commercial-off-the-shelf products in order to save development time, and they seek exemption from inspection because these components often contain proprietary content to which licensees may not be privy. It is therefore conceivable that vendors (and some are already considering doing so) may create voting systems nearly entirely composed of COTS modules, thereby circumventing much of the ITA process. This is especially problematic, given the lack of any way to recall later-deemed defective products (as noted above). There has been an ongoing attempt in the working group to include wording in the standard that would require inspection of COTS components that could directly affect ballot recording, casting and tabulation, but since segmentation of these units may be difficult to achieve, this has been met with considerable resistance.

Lack of Security Assurances: One large debate within the working group has involved the allowance for the use of transceivers (modems), especially wireless ones, within voting devices. Vendors state that they need these units for pre-election ballot face programming and post-election vote total collection, insisting "they can do this securely" while offering no assurances to voters or election officials regarding privacy and integrity. Another debate has involved whether cryptographic modules can provide adequate security and transparency for ballot collection. Here, vendor members have protested any insertion of requirements in the standard (such as a full mathematical proof of correctness of implementation) that would back up their assertions. Although a great step forward was made in the draft by requiring that software modules be digitally signed to prevent substitution, again no visible assurances of compliance were provided. An attempt was made to institute Common Criteria assessment at the EAL4 level, but the drafting of an appropriate Protection Profile became bogged down due to the necessity that the standard express only functional rather than design requirements. The lack of bona-fide assurances throughout the standard thus has a grave impact on provisions for security assessment.

End-to-End Omissions: This standard is intended to address only polling-place based ballot collection and tabulation devices. At the outset of the project, a decision was made to exclude ballot face preparation, access control, and precinct total aggregation components. Since some vendor products have reprogramming capabilities, down to the firmware level via data portals, any interfacing devices (such as ballot layout cartridges, voter smartcards, and end-of-day reporting systems) can pose significant risks that must be mitigated in some (as yet undetermined) fashion.

Auditability: Attempts to require independent auditability of fully-computerized voting systems via the use of voter verified paper ballots were resisted by many vendor members. Some of the cryptographic community attempted to obfuscate this issue through the distortion of the word "verified" into "verifiable" -- representing an electronically secured ballot image. This inappropriate wording persists in the draft.

In summary, this P1583 draft is not "ready for prime time" and must be cautiously considered only a "work in progress" since security and auditability issues are not adequately addressed. Beyond as an overview, I cannot recommend its use.