The FEC Proposed Voting Systems Standard Update
A Detailed Comment by Dr. Rebecca Mercuri
Submitted to the Federal Election Commission on September 10, 2001
in accordance with Federal Register FEC Notice 2001-9, Vol. 66, No. 132.

Background

In 1990, the Federal Election Commission approved a set of performance and test standards for voting systems. These standards were voluntary, and since their inception only slightly over two-thirds of the states have adopted them, so they have not been universally applied throughout the country. The earlier standards were criticized by concerned experts as having been heavily vendor influenced, as may be the currently proposed ones. This is evidenced by the inclusion of dubious technologies, and the lack of strict security assurance provisions, as well as other salient omissions.

In the meanwhile, voting systems continue to evolve, outpacing the abilities of local and state governments to adequately assess the equipment they are considering for purchase. There is an increasing, and potentially dangerous tie between vendors and municipalities, due to the ongoing maintenance required by computerization. That a "trust us" mentality exists is illustrated by the fact that proprietary hardware and software protected by trade secret nondisclosure is still the rule in election systems. Furthermore, many of the new products offer no independent audit trail, and some afford vast opportunities for global attack, vote selling, voter coercion, and disenfranchisement. Although election officials have long understood that every vote indeed does not count, and that all election systems carry some degree of error, the FEC has shied away from setting minimum performance benchmarks in this recent proposal. Sadly, the result is that communities with good intentions of replacing their current election equipment may very well find themselves purchasing new systems that are inferior to those they already own.

I have thoroughly examined the voting system standards proposal and present here my comments to the FEC in response to their Federal Register Notice dated July 10, 2001. Since the issues on which I have remarked are numerous and highly detailed, I would like to restate my earlier offer to discuss these matters in person with the appropriate FEC representatives, or in a public forum arranged by the FEC and/or NASED. In this way, it will be possible to better understand the failures of the proposed standards to address the concerns of municipalities hoping to provide the public with voting systems that maintain the accuracy and integrity that our elections demand.

Overview

The comments in this response have been organized to be consistent with the flow of chapters and sections in the proposed standard, although some topics may be found in multiple places in the FEC document. For the sake of brevity, I have limited my comments to certain topics which I feel are inherently flawed in the proposed standard. The ones addressed herein are as follows (with reference to the VSS update in parentheses): election standards (chapter 1), accessibility (section 2.2.5), internet use (section 2.4.3.4), software/firmware standards (chapter 4), telecommunications (chapter 5), security (chapter 6), quality assurance and configuration management (chapters 7 and 8), testing (chapter 9). I have also added a section addressing the matter of recounts. A brief resume and a list of suggested readings are located at the end of my response.

I have elected not to directly address considerable portions of the chapters on functional capabilities and hardware standards, in part because the comments which I have made about the other sections necessarily impact those aspects as well, and also because those sections have been written in such broad fashion as to allow wide variation in implementation. Any product must be assessed as to the components it includes, some of which may be in conflict with satisfactory voting system performance. If the FEC desires my comment on those chapters and other sections that I have not included here, I would be willing to present a more detailed review upon request.

Election Standards

As the United States Supreme Court indicated in the verdicts on Florida's election contest, the establishment of election standards is a matter of states' rights. In the absence of Congressionally enacted laws or a Constitutional amendment creating minimal requirements for Federal elections, the equipment that is used for voting (which typically will be the same as that provided for local or state-wide races) can differ from state to state, and further may even differ between and within counties in each state. Examples of such variant regulations include the casting of straight-party ballots, the admission of blank (no-vote) ballots, the use of full-face ballots and other ballot layout formats, and the tabulation of proportional rather than highest vote results. Such differences are mentioned in sections 2.2.6, 2.3.1.2, and elsewhere in the proposed standard document. The laws pertaining to resolution of contests through recount processes also present a high degree of variation.

Voting system vendors are thus faced with the daunting task of providing variously configured systems in order to conform to these conflicting requirements. Each of these configurations and processes must be independently verified by the testing authorities. Manufacturing organizations are not accustomed to this -- they tend to create products that (more or less) serve the needs of an application area generically, and features are grandfathered to permit future use without modification -- a good example is that of the automobile industry, where laws regarding passenger restraint systems or headlights are adopted into all products, not different ones for each state and city. For voting, the proper maintenance of multiple, incompatible product lines necessarily would require the implementation of sophisticated tracking systems, difficult to achieve in the computer industry, especially for vendors with limited resources and manufacturing experience.

Such matters become critical when laws change, or defects are noted and product recalls become necessary, yet the proposed standard does not adequately address how the FEC intends to track and report such alterations and problems to municipalities with similar (but not necessarily identical) equipment. Nor does the proposal examine the multitude of difficulties presented by recertification of modified products, or the impact of such modifications on functionality. Since it does not appear likely that a generic set of voting regulations will be adopted throughout the country, issues related to system incompatibilities will likely persist for the foreseeable future.

Section 1.1 of the FEC proposal states that "The standards specify minimum functional requirements, performance characteristics, documentation requirements, and test evaluation criteria. Essentially, they address what a voting system should reliably do, not how the system should meet this requirement." The task of providing a standard intended for broad use, by multiple audiences, serving various needs, results in a document which is too general for applicability. Where it most fails in its purpose is by shying away from the establishment of true minimum benchmarks, by not insisting on specific controls for security, functionality and verification, by not delineating techniques for ensuring that ballots are ergonomically prepared, and by not precluding the use of features known to be deleterious to election processes. Some of these matters will be further elaborated below.

Accessibility

Although it is admirable that the proposed standard includes sections (such as 2.2.5) on voting system accessibility, there appears to be a general conclusion that all procured systems must be ADA compliant. For example, some municipalities are currently being forced into the adoption of EVT kiosks when they would rather use optical scanning, because the paper-based systems are not accessible to the visually impaired, and their state laws do not permit the use of multiple technologies within the same district. This could be analogous to requiring building facility accessibility and insisting that all persons use these ADA features (i.e. everyone has to take the elevator). It is conceivable that a broad range of potentially costly accessibility features may be thus imposed on new voting products adopted for use. Rather than create blanket requirements, communities should be allowed to purchase systems that are outfitted to accommodate the percentages of disabled and non-disabled populations served, and they should be permitted to deploy these

systems in ways that will best encourage enfranchisement. The proposed standards should reflect this understanding.

Internet Use

The Internet poses one of the largest risks to the accuracy, integrity and security of voting systems to date. The current status of the Internet is that **all** servers (and the systems attached to them) are subjected to attack, many on a constant basis. Prevention mechanisms are "after the fact" -- typical modes of invasion are avoided through remedies following detection. Attacks can be performed locally by persons who have system knowledge, or globally by individuals or groups who may escape prosecution through loopholes in international law. ***There is NO KNOWN WAY to eliminate the risk of new forms of Internet system penetration.*** There is also no way to determine whether backdoors exist in standard products such as the operating systems and compilers that are used to develop and run voting systems. Internet attacks have already cost the computing community billions of dollars due to time, information, and services lost, with no promise of solution. Illicit penetration of election board computer systems has already occurred. Attacks aside, there are many other unresolvable issues related to the use of the Internet for voting systems. These include (but are not limited to): monitoring, coercion, vote selling, disenfranchisement, on-screen advertisement, and system and software incompatibilities.

There is a gross underestimation by the FEC of the difficulties of Internet usage. This is apparent when perusing section 2.4.3.4 on Internet Voting Systems Standards. Some of the points there indicate that: voters should be identified by passwords; ballots should be encrypted; high-bandwidth connections should be available to support peak activities and defeat denial of service attacks; test ballots should be cast to verify end-to-end integrity; and so on. All of these statements have serious flaws, as follows: voter passwords could potentially be used to track ballots cast, thus violating anonymity; cryptography can not provide sufficient assurances of privacy or correctness; it is impossible to anticipate the extent of denial of service attacks nor to estimate its effect on voter confidence and election results (disenfranchisement targeted to certain vicinities could alter an election outcome); and the use of test ballots does not in any way assure proper functionality. Extensive material on these and other pertinent topics is available within the computer science literature.

It is therefore a grave mistake for the FEC to include even the future possibility of Internet usage for ***any*** aspect (balloting, result reporting, reprogramming, voter authentication, etc.) of voting system implementation. All references to Internet usage should be removed from the proposed standard. A strong statement regarding prohibition of Internet usage in election systems should be added.

Software/Firmware Standards

Chapter 4 of the proposed standards document addresses software and firmware related issues. Various major security loopholes are created in the exclusions section 4.1.4 (and in other exclusions in the proposed standard), first by allowing additional non-voting-related software to reside on systems being used for voting, without requiring assurances that the voting system cannot be affected by concurrently running programs, operating systems, and the like. Another significant weak link in voting system security is permitted by the statement that "Commercial software will not be subject to code review." Since it has been often demonstrated (as early as 1984 by Ken Thompson in his classic "Reflections on Trusting Trust" lecture which illustrated the manner in which a compiler can be easily rigged to generate Trojan Horse software, without any trace in either the compiler sourcecode, or the sourcecode of the programs being compiled) that standard products should not be assumed to be free of errors or trustworthy, this is a dangerous omission by the FEC. All software/firmware as well as the processing chip set should be subjected to examination, whether proprietary, generic, or specific to the voting application.

Chapter 4 further discusses audit records. Here the proposal requires the use of audit trails in order to provide independent verification of computer processes and data. Voting differs significantly from other application

areas (such as banking) where audit trails have been used, due to the simultaneous requirement for anonymity in balloting. In banking, say at an automated teller kiosk, there are various monitoring systems in place -- cameras, keypress logging, time stamps on transactions, paper receipts, accounting for cash deposits and withdrawals, use of access cards and pins for identification, and so on. When these tracking systems fail (and they do, billions of dollars are lost through identity theft and other banking system compromises each year), the banks are covered by insurance, re-insurance, and federal insurance programs. The same is not true for voting. Voting must be performed without receipts (or vote selling would be encouraged), and the transactions with the voting system must not be recorded sequentially, or even in their entirety, or anonymity will be violated. In voting, there is no compensation for losses in the event of election system failure.

The vendors of EVT kiosks and Internet voting systems have proposed randomization and encryption of ballot images for protection, but the fact is that ***these schemes can not ensure that the ballots cast by the voters are the ones that have been recorded, transmitted, and/or tallied***. As Roy Saltman stated in 1988, "the voter is given some reason to believe that the desired choices have been entered correctly into the temporary storage, but no independent proof can be provided to the voter that the choices have, in fact, been entered correctly for the purpose of summarizing these choices with all others to produce vote totals." This statement is still true, and it is true whether the choices are entered into temporary or permanent storage modules. There is simply no way, in an anonymous election, to use a fully-electronic process that is independently auditable. Systems using these schemes have failed in actual elections, votes have disappeared or in some cases even been transferred to other candidates tallies, and the vendors have not been able to recover the actual ballots cast. This may be due to defects in hardware or software, improper programming of ballot configurations, or nefarious actions.

The FEC chose to ignore Roy Saltman's admonishments in the 1990 standards document -- had they not done so, the situation in Florida 2000 could have been averted by requiring certain changes in the use of punch card systems. It is unclear why, at this critical juncture, the FEC has chosen to ignore this most critical flaw in the new electronic technologies, but it must be addressed.

One solution to the disappearing electrons problem is to require that all fully-electronic balloting systems provide a physical audit trail that is human-readable. The simplest such mechanism involves the production of a printed ballot (or printed list of voted selections). This would be perused by the voter and then deposited (possibly within a protective enclosure to prevent alteration) into a ballot box. The ballots thus produced would be considered the actual record of the election (other EVT totals would only be used to provide preliminary non-official results), which would be recounted through OCR technologies or manually, under bipartisan (or multipartisan) overseeing.

Although many have objected to the use of paper as a component of election systems, recent studies (by MIT/ CalTech and others) appear to point to paper-based (hand counted or optically scanned) as more reliable than electronic systems. A paper ballot, readable by the voter, is the only way to place verification into the hands of the citizens who are participating in the election. Voter confidence should thus be increased. The ability of third-parties (such as press agencies, the League of Women Voters, and research organizations) to independently re-verify the election from the materials that voters actually used, is also an important part of the post-election process, and must not be ignored. Paper may eventually be replaced by other balloting mechanisms, but since there is no present technology that can suffice in this regard, it is imperative that the FEC standard include paper ballot production for all fully electronic systems so that independent verification can occur.

Telecommunications

Telecommunications poses risks that are similar to those involved with Internet voting systems. Reliance on an external network for services essential to conducting an election means that security, reliability, durability, maintainability, privacy, response time, and other aspects may not be assurable. Add-ons, such as encryption

and digital signatures, are inadequate since even though the ends may be secured (which is not necessarily the case), the vulnerability of the middle (transmission system) creates a severe security flaw. Interestingly, the FEC proposal contains an implicit admission that the telecommunications medium is insecure when, in section 5.3, it "prohibits the transmission of specific types of voting-related information via telecommunications due to the limits of existing technology to prevent unauthorized access and use of data." Either the medium is secure, or it is not. Remedies that would be insufficient for certain communications are in fact insufficient for all. This inconsistency needs to be addressed.

Security

Although the United States has an existing program for providing computer security assurances, mandated by the Congressional Computer Security Act of 1987, the FEC has not chosen to apply this standard to election equipment, despite the fact that it processes "sensitive information" whose "loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs." For the last decade, computer security experts have urged members of the FEC, state and municipal election officials, as well as voting system vendors, to require or voluntarily subject voting systems to the security assurance program administered by the National Institute of Standards and Technology. Their earlier Trusted Computer System Evaluation Criteria (TCSEC), its international superset, the Information Technology Security Evaluation Criteria (ITSEC), and their recent replacement, the International Standards Organization Common Criteria (CC) represents the best security review that the computer industry provides. To date, absolutely no voting system has been subjected to this form of scrutiny, even though it is routinely applied to other products, most typically those used by the Department of Defense, but also voluntarily within health care and other industries where security is a concern.

The FEC voting system security standards, as described in chapter 6 of the proposal document, are both vague and weak. They do not even begin to address the multitude of interacting and interdependent components requiring analysis and control in computer systems. I have performed a detailed analysis of voting system features that would be required to be examined in a Common Criteria assessment. This analysis covers such items as: system requirements, functionality, correctness (accuracy), accountability, disclosability, reliability, integrity, availability, fault tolerance, data requirements, confidentiality, retention and recountability, user requirements, adminstrator requirements, interface usability, documentation, testing, paths, facility management, recovery, system distribution, and compliance with laws and regulations. The analysis concludes that minimally a CC level 4 assessment should be required for voting systems. Components of systems that rely upon sophisticated algorithms for security may even need to be assessed through provability analysis at level 7. My analysis further includes lists of questions that should be replied to by all voting system vendors as a portion of the security analysis. Information regarding my analysis has been offered to the FEC and is available upon request.

The omission of acknowledgement and use of the Common Criteria program for security assurances in voting systems means that either standards that are below those used for other computing applications will be administered, or that a different set of standards created by the FEC (possibly incompatible with the CC, posing difficulty for general-use components such as operating systems) may be required to be applied for NASED approval. Both of these situations are unacceptable. The two decades of research and experience by NIST in its computer security assurance program must be acknowledged and used by the FEC and NASED, as well as adopted by the states in their voting system security assessments.

Quality Assurance and Configuration Management

The Quality Assurance and Configuration Management measures described in chapters 7 and 8 of the proposed standard represent a sound industrial approach to such matters. Idealistically, these measures would be applied to the production, deployment, and maintenance of voting systems through cooperation between the vendors, testing authorities, and municipalities. In reality, most municipalities (except for the larger cities) lack

the technical expertise to be able to independently verify that the proper assurances have been made and that compliance has occurred. Testing authorities have limited resources for tracking these widely varying products through their manufacturing and deployment stages. Essentially, this leaves open questions as to how release updates will occur, how localities will know that the system delivered is the same as the one approved, how recalls will be tracked through notification reports, and so on. Lacking a overseeing authority with the ability to impose global control over election system configurations, the QA and CM measures thus described are hardly likely to be effectively applied. The FEC and Congress need to enact laws which will fund such centralized efforts so that communities can obtain assistance and guidance in their efforts to enforce these controls.

Additionally, QA and CM generally pertains to products as delivered, and maintenance that is performed by the vendor. The issue of how computer-based products will be maintained by the local election boards in such fashion that they are not tampered with or corrupted during the long months of storage between elections, is not adequately addressed by chapter 3 of the FEC proposed standard.

The computer industry is currently in a state of flux -- companies come and go, and product lines may not continue to be supported. QA and CM do not sufficiently address how municipalities using computerized products will be protected from obsolescence due to unavailability of components, discontinuation of product lines, and dissolution of companies. Voting systems may be required to be scrutinized in legal actions related to recount contests, and information regarding product internals may be withheld due to security or trade secret issues. Some election boards have already experienced litigation due to product failures, and this is likely to increase as computerization continues. QA and CM (as well as testing and documentation) must be sufficient to resolve claims of product defects and tampering which could appear in liability and reliability lawsuits. The FEC proposed standard falls short of providing a comprehensive collection of voting system evidence that can be used by municipalities in the event that such disputes occur.

Testing

The recommendations embodied in chapter 9 of the proposed standard primarily consist of functional testing and documentation reviews. This is what is known as a black box assessment. Black box testing can only assert that the product seemed to function correctly under the constraints of the examination (using the data sequence provided at the time of the evaluation) and it does not reveal anything about other operations which could exist and be triggered within the voting system during actual use. The related white (or open) box testing (such as system analysis, circuit design and code reviews), which is typically performed in conjunction with or in addition to functional testing as an industry standard has been omitted from the recommendations for ITA reviews. Well documented studies reveal that white box testing can detect further significant errors, many of which can not be found through functional testing alone. Such extensive reviews would be both time-consuming and costly, but are essential, especially if the vendors are allowed to hide the details of their implementations from the public. Concerned scientists have been recommending white box testing for voting systems for many years, yet the FEC has continued to ignore the necessity for this type of examination.

The documentation review suggested in the proposed standard focuses on that which has been submitted by the vendor, and does not address the additional documentation (for procedures, training, operations, maintenance, and use) that is provided to or generated by the municipalities where the systems will be deployed.

Recounts

An extremely serious omission in the standards proposal involves the mechanisms and procedures for dealing with recounts. In the Florida 2000 election matter, the nature of the recount (how it should have been performed and the laws pertaining to its resolution) were as much (if not perhaps even more) of an issue as were the systems used to cast and tabulate the votes. The statements in section 2.2.2.1.1 pertaining to

accuracy, specifically that "All systems shall: Record each vote precisely as cast and be able to produce an accurate report of all votes cast" is not attainable by any voting system. ***All voting systems carry with them some degree of error***, and this error must be accommodated in the regulations pertaining to system performance.

Statistically speaking, when there is a degree of error, and the differentiation between choices falls within this error, a "dead heat" (or tie) should be reported. It should no longer be considered acceptable for communities to count and recount the votes, coming up with different answers using various methodologies, while clinging to the erroneous belief that a result that favors one candidate above another within the degree of error for the voting system actually should be used to proclaim the winner. A tie should be declared, and a runoff among the tied candidates should occur through a new election contest. The FEC is negligent in not establishing minimum performance benchmarks in this proposed standard, since they are well aware that at least a 2 percent error is common across all voting systems, and since this error must be accounted for in any recount contests.

Conclusions

In short, the proposed update to the Voting Systems Standards by the FEC fails to provide an adequate "vehicle for state and local election officials to assure the public of the integrity of computer-based election systems." In particular, its major flaws are that it **does not** effectively address the:

- varying and sometimes inconsistent or incompatible state and municipal regulations;
- lack of true minimum benchmarks for system performance;
- absence of techniques for ensuring that ballots are ergonomically prepared;
- allowance for specialized products which will aid a variety of disabled populations;
- elimination of the use of features (such as the use of the Internet) known to be deleterious to election processes;
- improper exemption of auxiliary software from certification examination;
- necessity for physical verification of ballots in order to ensure that the votes cast are indeed the ones that have been recorded, transmitted and tallied;
- risks involved with reliance on telecommunications services in election products;
- necessary application of existing ISO and NIST security standards to voting systems;
- establishment of shared expertise bases so that municipalities can assure that quality assurance, configuration management, deployment, storage, training, maintenance, use, and update requirements are met;
- inadequacy of functional (black box) testing for computerized voting products;
- need for recount regulations that involve recognition of inherent degrees of error.

All of these issues are either absent from or improperly handled by the currently proposed FEC standard. It is crucial, at this juncture in American political history, that the FEC obtain the assistance of independent experts who can assist in producing a viable standard for computerized voting systems. The proposal is a good framework, as it sets out the many topics which require consideration in elections, but considerable work needs to be done before this document will be able to satisfy its stated purpose.

Resume

Rebecca T. Mercuri has been actively involved with the assessment of voting systems since 1989. A specialist in interactive systems and forensic computing, over the last two decades she has worked for such firms as Intel, AT&T, RCA, Merck, and SRI as well as such agencies as the Department of Defense, the Federal Aviation Administration, the Philadelphia Stock Exchange, and many other small and mid-sized businesses and corporations. Rebecca Mercuri holds a Ph.D. and a Master of Science in Engineering from the University of Pennsylvania's School of Engineering and Applied Science, along with a Master of Science in Computer Science from Drexel University. She is the president of the consulting firm Notable Software, Inc., and an assistant professor of computer science at Bryn Mawr College.

Dr. Mercuri has written numerous papers (some with the noted risks expert Dr. Peter Neumann of SRI) on the subject of electronic vote tabulation, and has provided testimony for the Florida recount to the 11th Circuit Court of Appeals (which was referenced in one of the briefs to the U.S. Supreme Court), testified before the U.S. House of Representatives Science Committee regarding the need for stronger standards in elections, and advised the U.S. General Accounting Office on this matter. Other testimonies have included the New York City Board of Elections, the Pennsylvania House of Representatives, and the Houston City Council. She maintains an extensive website on electronic voting and is anticipating publication of her Doctoral Thesis entitled Electronic Vote Tabulation Checks & Balances. Dr. Mercuri has received awards from the national Association for Computing Machinery and the Institute of Electrical and Electronics Engineers for her service to these organizations.

Rebecca T. Mercuri, Ph.D.

http://www.notablesoftware.com
mercuri@acm.org

References

This section is not intended to be a comprehensive list of references, but includes those most pertinent to the topics addressed by this document.

CalTech/MIT Voting Technology Project, *Voting: What Is, What Could Be*, July 2001.

Common Criteria Implementation Board, *Common Criteria for Information Security Evaluation*, ISO IS 15408, 1999.

Mercuri, Rebecca, *Electronic Vote Tabulation Checks & Balances*, Doctoral Dissertation, University of Pennsylvania, School of Engineering and Applied Sciences, 2001.

Mercuri, Rebecca T., *Physical Verifiability of Computer Systems*, 5th International Computer Virus and Security Conference, March 1992.

Neumann, Peter G., *Computer Related Risks*, Addison-Wesley, 1995.

National Computer Security Center, *Department of Defense Trusted System Evaluation Criteria* (TCSEC), DOD-5200.28-STD (Orange Book), December 1985.

Saltman, Roy, *Accuracy, Integrity and Security in Computerized Vote-Tallying*, U.S. Department of Commerce, National Bureau of Standards, NBS Special Publication 500-158, August 1988.

Schneier, Bruce, *Secrets and Lies: Digital Security in a Networked World*, John Wiley & Sons, Inc., 2000.

Thompson, Ken, *Reflections on Trusting Trust*, Communications of the ACM, Volume 27, Number 8, August 1984.