Before the

United States Election Assistance Commission

In the Matter of

Testing and Certification Program Manual 2006

COMMENT

By the Fair Elections Committee of Democracy for New Hampshire[1]
And Election Defense Alliance[2]

John A. Carroll[3] and Nancy Tobi[4], authors

Introduction

The Commission is to be commended for inviting public comment on this matter. We will be raising some uncomfortable thoughts, which may run counter to commonly held beliefs. We consider this necessary to arrive at a sound policy.

Most of the Certification manual deals with administrative and legal details, which we will come to later in this paper. First, we will be discussing more substantive issues, chiefly the question of whether computerized products are at all appropriate for use in our elections, the manner in which voting equipment would have to be regulated, how its design would need to be shown to be correct, and whether any types of voting equipment are compatible with the secret ballot and therefore worth the Commission's resources to regulate. Assumptions in those subject areas underlie material in this manual; therefore we consider these topics relevant to the matters under consideration.

Certification Premises, Assumptions, and Procedures

Computerized voting equals secret vote counting

First we raise the question of whether or not it is appropriate at all to use computerized voting equipment, of which the processes are unobservable, and therefore constitute secret vote counting mechanisms. The basis of a free and open democracy such as that defined in the United States Constitution, the Voting Rights Act, and other State documents, relies on open, observable, and transparent election procedures, especially with respect to voter intent and vote counting. The use of computers to fulfill the function of marking ballots and then counting the votes nullifies this basis. Even computerized systems offering “open code” solutions violate the basis of open and transparent vote counting procedures, because while one can see the code, one can not see the counting that occurs within the computer program.

Given this obvious contradiction between the requirement for observable vote counting and the impossibility thereof with computerized voting equipment, we suggest that the entire certification process is moot. We strongly encourage the EAC to look towards more democratic election methods and procedures, and we support any efforts in that direction.

Nonetheless, because we have in existence a multitude of computerized voting equipment throughout the nation, we have reviewed the manual in its entirety and offer consideration of the manual and its contents in the remainder of our comments.

[1] www.DemocracyForNewHampshire.com

[2] www.ElectionDefenseAlliance.org

[3] 77 Musket Dr. Nashua, N.H. 03062 mykrowatt@comcast.net

[4] 28-31 James Street, Milford, NH ntobi@tds.net

EAC certification processes do not fit real world application and needs

The entire model defined within the certification process must be rethought as to its real world applicability and feasibility. The EAC itself has made a tacit recognition of this dichotomy in its recent decision to only implement its full program for 2006 in December, after the elections will have been held, and after the critical time when that program would have actually been relevant and meaningful.

With its decision to implement the full 2006 program only after the elections are held, one has to question the efficacy of developing testing guidelines and standards if they are never to be actually implemented in the real world in a manner to be relevant to the needs they purport to fulfill. If waivers and grandfathering of equipment and test labs is to be the norm, then it seems irresponsible to continue to pour taxpayer funds into a well that can never be tapped.

Under this scenario, the certification process itself is rendered moot, which most likely explains why so much of the manual is dedicated to finding ways to work around the process.

We must recognize that even under a conventional commercial model, software development takes a long time and a lot of money. And even when the final product is released to the market place it is inevitably full of bugs. Typically, on the commercial market, software companies continue to develop their product even after it has been released and sold on the public market. They simply send out updates and "patches" to take care of the bugs that their customers encounter and complain about. That's at least somewhat tolerable in the commercial world, where the risks are merely monetary and losses can be insured against.

Elections, on the other hand, are held at fixed times every one, two, and four years. They cannot wait for software to be debugged. Elections are constitutionally mandated core governmental functions, which must be conducted accurately and in a verifiable manner. Elections are public events, administered by elected officials and financed by the public. Elections guarantee the continuation of the Republic. The risks created by unproven software and equipment are not tolerable at all.

Regulatory approach

A fundamental problem with the processes described in the manual is the regulatory approach toward complex voting equipment. To date, these machines have been treated in a manner similar to commercial data processing equipment. In fact, on January 19, 2005, the Technical Guidelines Development Committee (TGDC) made a conscious decision and recommendation to view the standards and testing procedures according to commercial rather than military standards. This decision unaccountably altered the approach of the TGDC and the EAC from that of national security—which, of course, is an appropriate approach for anything having to do with the nation’s elections—to that of a commercial market enterprise for profit and gain.

We suggest that any serious exploration of election equipment regulatory activity would have had to be viewed in terms of national security and safety-critical devices. This would require radical changes in design philosophy, Commission rules, and approval procedures. In particular, testing, which this manual speaks of, would have been replaced by risk analysis, Failure Mode Effects Analysis (FMEA), and formal code review.

We justify this by pointing out that the consequences of a misreported or miscounted election can be exceptionally severe. The loss of life and property can be much greater than the result of malfunction in an airliner's flight controls or a power plant's boiler safety interlocks. The voters are responsible for determining who can be trusted with authority; overriding their decision and putting the wrong people in office can result in breakdown of the rule of law, financial catastrophe, war, or worse. It is not sufficient to reduce the probability of logic flaws to a low level by sequential testing and debugging; it is necessary to prove conclusively that no critical bugs exist. When the Federal Aviation Administration (FAA) or Underwriters Laboratories (UL) permit safety-critical devices to be put into service, they don't rely on testing to uncover subtle flaws. Rather, they require that the effects of every component failure which is physically possible be examined, and shown to result in a safe condition. Similarly, safety-critical software is not verified by testing, it's verified by comprehensive analysis at every level of design detail, to show that no safety-critical logic faults exist.

There are well-established published standards for design correctness in these types of hardware and software, and there are experienced engineers and agency personnel to apply them. In aviation, software is developed and verified according to the quality discipline of RTCA/DO-178B, and hardware comes under the companion standard RTCA/DO-254. UL evaluates industrial safety-critical software according to UL 1998; hardware for different applications is covered by a variety of different standards.

Further advances in design integrity are under way in the academic community. For example, at the University of Texas and other institutions, progress has been made in the formal proof of correctness of both software and hardware logic design[5]. (When we speak of "proof" in this context, we don't mean the "proof beyond a reasonable doubt" that prevails in jurisprudence. We mean the absolute and final proof demanded in the world of mathematics. Because a computer program or the hardware logic of a computer's processing unit are purely logical constructs, it is possible for them to meet this rigorous standard of proof. What remains is the physical-world possibility that the hardware may fail because of defect or damage, and that requires a comprehensive FMEA.)

An important point to realize about both provably correct design and fail-safe design is that they demand extreme simplicity, to reduce the verification problem to manageable proportions. A piece of equipment must be designed from the ground up to be fully analyzable; FMEA and proof of correctness can't be tacked on after the fact. Thus, off-the-shelf computers and off-the-shelf operating systems can't be qualified for these critical systems. Typically, the application itself runs on the bare hardware and interacts directly with the physical components to ensure that the failure modes are fully predictable and safe. Even so, the long and arduous nature of the design discipline and the verification process severely discourages design changes; this puts a premium on getting the requirements correct before starting. This type of hardware and software isn't successively improved; it has to be fully correct to be released at all.

The Commission has relied in the past on technical assistance from the National Institute of Standards and Technology. NIST is one of the world's foremost institutions in metrology, but the validation of voting equipment design is not a problem in precision measurement. We suggest that the Commission draw on the resources of regulatory agencies and private organizations that have direct experience regulating and approving safety-critical products.

While standards such as UL 372 don't apply directly to voting equipment, they contain much in the way of experience-tested principles and language that could be used in new standards for these devices. In particular, UL 372 mandates fail-safe design and details its requirements. This is particularly relevant. Flame safety controls, like ballot counting machines, belong to a category of safety-critical devices in which a safe shutdown is possible.

A safe failure of a ballot counting machine can be defined as one which doesn't indicate an incorrect result without also giving an unmistakable indication of failure. In that situation, the result is discarded and the ballots are counted by another machine or by hand.

If the Commission were ever to identify a solution other than hand counting, which met the requirements of observable and transparent vote counting, it would at the very least also need to apply security- and safety-critical standards and testing methods to its certification process.

Recognition of commercial market forces versus national security

A distinction must be made between developing software and hardware products for the general commercial market versus safety-critical products for important public purposes, and in particular when those products influence the safety and security of the American Republic. On a number of levels, the proposed certification guidelines and procedures do not seem to recognize or acknowledge this distinction.

1. Neither in the Application for Certification (Appendix A & B) nor in any other section of the manual do we find reference to the critical nature of voting system equipment. The certification manual does not include any requirements for security procedures and clearance of any and all personnel engaged in the design, development, production, and distribution (in short, the entire supply chain and life cycle), of election equipment. Neither does it propose to mitigate personnel and organizational security risks by

[5] A Google search for "software proof of correctness" produces numerous hits.

approving the engineering drawings and source code in an open, public regulatory action at the end of design, as we propose for New Hampshire. We would not imagine such an oversight for other products on which the safety and security of the nation depend, and we object to its absence here.

2. The certification manual gives inordinately wide latitude for manufacturers seeking to circumvent the certification process. Some examples of this are described below.

   2..a Emerging technologies (Section 3.2.2.4) seem to be allowable even though they cannot be tested under any agreed-upon guidelines.

   2..b Section 3.5 seems designed specifically to allow manufacturers to market their products in the absence of adherence to EAC guidelines and NIST testing standards. This approach of providing waivers that expire after the election and after the equipment has been used during that election, undermines the very purpose of the certification process: that only tested and certified equipment be deployed in the nation's elections. It is a contradictory and unacceptable approach to favor expedience over national security. If products cannot meet certification standards then they must not be deployed. As noted elsewhere in this document, there are acceptable alternatives to a technology-driven election system when that technology-driven system is proven to cause a risk to the safety and security of the American Republic, its people, and the democratic processes that are its foundation.

   2..c Similarly, Section 4.4.2.3 provides unacceptable latitude for system modifications. We suggest that system modifications in a product such as this demand that the system undergo full and complete recertification testing to ensure that the overall previously-certified product integrity remains intact despite the modification.

3. The exemption of COTS elements from the certification process provides a huge security hole and serves to undermine the integrity of the overall process as a result. It is unacceptable to waive commercial products embedded in voting equipment from the same process of scrutiny and testing that every other element must undergo.

Openness and verifiability

Here, we write from the background of New Hampshire election law. New Hampshire has some of the most trusted elections in the country. A major reason is that our laws and practices are founded on openness and verifiability. Our statutes require that ballots be counted in public view at the polling place, immediately after the polls close. Inspectors appointed by the opposing political parties and issue advocacy organizations are an integral part of the process. They participate directly in the counting and cross-checking.

No secrecy whatever can be tolerated in the vote counting process. Thus, it is improper to consider schematics, source code, or any other part of the logic of an electoral machine as a suitable subject for trade secrets or any other kind of secret, as this manual does. Similarly, it is impossible to attain true openness in the vote counting process when that counting is being done in invisible bits and bytes inside a computer.

Computers are appropriate for all manner of things commercially, and with respect to our national security. The differentiating factor here is the requirement for openness and observability. It will be pointed out, and has been, that machine vendors will object strenuously to our position. Our position is that we don't care, and it matters not to us whether they remain in business. As citizens, we can't afford to care. The future of our country is at stake, and we must, as patriotic citizens, demand the cessation of factors contributing to the destruction of our democratic processes.

Elimination of vote recording machines

The elephant in the middle of the room that everyone has been tiptoeing around is the irremediable fallacy of vote recording machines. These machines are responsible for widespread voter disenfranchisement, as we have seen in recent years when insufficient numbers of vote marking machines led to long voter lines and many people simply leaving without voting at all. Other problems with vote marking machines are such that no amount of regulation or engineering can compensate for them. We urge the Commission to abandon all further efforts to certify vote recording machines, electronic or otherwise, and concentrate its equipment certification efforts on optical-scan ballot counting machines.

Here's the reasoning:

The nature of the secret ballot, which is essential to our system of representative government, is that an error in recording the vote is unrecoverable. If the voter can't detect the error and correct it while still in the voting booth, there is no possibility of detection and correction later. To use engineering terminology, the vote recording step is a single point of failure; thus ironclad reliability is essential here. This is completely unlike the situation with the automated teller machines on which much of vote recording equipment is modeled; there, a system of accounting checks and monthly statements closes the loop around the data collection step.

That being the case, the only way the voter can tell with absolute certainty that the vote has been recorded correctly is to see it on the ballot. Consequently, the only acceptable way to record a vote is in the form of human-readable marks on a durable paper ballot that can stand up to counting and re-counting without damage. And the only way to ensure that the vote the voter saw is the one that is counted, is to require the ballot counters, whether human or machine, to read those *same* marks. Therefore those human-readable marks must be the *only* form in which the vote is recorded.

For exactly those reasons, the New Hampshire legislature long ago passed a law stating that no machines can be used in the State unless they are able to read the voter’s choice on a paper ballot. This law was clarified this year to require that all votes to be recorded on paper ballots. Two Fair Elections Committee members, who serve in the legislature, helped bring that about. The ballots themselves, not the tally sheets, are the legal record of the election. The standard for interpretation is the voter's intent, and not conformance to instructions. Partly for those reasons, a second new law requires that all recounts be conducted “by direct inspection of the ballots, without electronic, mechanical, or optical devices.”

Since the requirement that all votes appear only in human-readable form on paper ballots is a matter of both logical necessity and statute, any economic justification for the existence of vote recording machines evaporates. A voter can't mark a ballot any faster with a $5000 machine than with a 50-cent pen. The machine can't save any time for the election officials, who must wait until the polls close in any case before counting the ballots. And, the machines have been known to malfunction and refuse to mark the ballot as the voter commands; a hand-held pen isn't capable of malfunctioning in that way, because it has no internal logic or memory.

Furthermore, just as you would not use a machine to sign a marriage contract, or any other contract of commitment, citizens, with their hand marked paper ballots, sign their commitment to their community. Human counters reciprocate this commitment to community by reading the voter intent as indicated on the ballot.

The economics of vote recording machines have always been questionable in any case; they have to be bought and maintained once per voting booth. This has been reported to cause major problems in some jurisdictions, where not enough money is available for the number of machines needed to handle the voter traffic. Simple curtained voting booths are much more affordable.

There is also the growing public uproar over electronic voting machines to consider. The many spectacular failures, the lack of visibility of the internal design and programming, the strange discrepancies between official results and exit polls, and the discovery of vulnerability to tampering and lax security are causing a fully justified skepticism as to the accuracy of machine-recorded election results.

To be perfectly blunt, we consider the arguments for vote recording machines on the grounds of accessibility for the blind and the illiterate to be dishonest, and a disingenuous excuse to push these machines into all polling places in order to maximize vendor profit. There are ways for these people to vote without subjecting the whole electorate's votes to the risks of vote recording machines. Furthermore, the possibility can't be entirely ruled out that the real reason to promote these machines for general use, with their invisibly recorded votes, is to facilitate undetectable election fraud on a massive scale. But whether criminal intent exists or not, the wide and growing suspicion is undermining the legitimacy and authority of representative government. That erosion of public confidence is dangerous in itself. The conspiracy theories will never go away until the vote recording machines go away.

Even if vote recording machines were to be developed according to safety-critical design standards, only specialists would be able to fully understand and verify the proof of correctness. That would still leave the general public uneasy. A simple pen, on the other hand, operates in plain sight. Anyone can use it and determine whether it's working correctly.

Optical scan counting machines

As an interim solution for those locales that do not yet have the infrastructure in place to support 100% hand counted paper ballot elections, optical scan ballot counting machines are a different proposition.

Their errors are recoverable, provided they're detected. There are measures that can be taken to improve detection, such as precinct level manual verification audits, so that the machines need not be fully trusted. Running a ballot through a scanner doesn't do anything to the ballot; it can be run through again, or counted by hand. As well, only one machine is needed per polling place, so the costs and risks of voter disenfranchisement are lessened.

Near-term solutions

One policy change that's urgently needed is an end to quick fixes. Meanwhile, it's still necessary to conduct elections correctly and on time, and have them seen to be conducted correctly. The only short-term solution is the proven method of hand-marked, hand-counted paper ballots. New Hampshire has had 300 years to fine-tune that process. It's fully laid out in our laws[6] and our election procedures manual[7]. New Hampshire is not the only jurisdiction that conducts elections with integrity and efficiency, but it's the one we're acquainted with. The Commission would do well to examine our election systems as a model for rapid emulation elsewhere.

We're aware of the 1934 book “Election Administration in the United States,” available from the Commission's web site, and in particular the methods of committing fraud with paper ballots described in chapter 9. We're not persuaded, as the author is, that substituting machines for paper ballots prevents fraud; on the contrary, it simply substitutes different opportunities for fraud, and does away with a physical record that can be produced for recounts and judicial appeals. Rather than jumping from the frying pan into the fire, New Hampshire has faced paper-ballot fraud head-on with carefully written laws developed over a period of centuries.

Opportunities for Commission action

Given that the Commission's mission is to assist states and localities to improve the integrity and efficiency of their elections, it's worth asking what actions can be taken in the short term to achieve real improvements.

The gold standard is the hand-marked, hand-counted paper ballot. Some election officials have become convinced that manual counts are beyond their resources. One action the Commission could take is to identify some of the most effective and efficient local election officials, and document and publish their methods. Even in New Hampshire, some moderators are able to teach their teams to complete their tasks much more quickly and economically than others.

Another opportunity for useful near-term action would be an accountant's analysis of the labor costs of the most efficiently conducted hand counting operations. Some preliminary investigations conducted here suggest surprisingly low costs, at least when efficient methods are used.

It would also be possible to organize training for state and local election officials in the best practices for managing open and verifiable elections with paper ballots. State legislators and local officials should be informed of the alternatives available.

[6] http://www.gencourt.state.nh.us/rsa/html/nhtoc.htm Title LXIII
[7] http://www.sos.nh.gov/FINAL%20EPM%208-30-2006.pdf