ACCURATE

A CENTER FOR CORRECT, USABLE, RELIABLE, AUDITABLE, AND TRANSPARENT ELECTIONS

Public Comment on the Manual for Voting System Testing & Certification Program

Submitted to the United States Election Assistance Commission

October 31, 2006

Prepared by the Samuelson Law, Technology & Public Policy Clinic
University of California, Berkeley

ACCURATE Principal Investigators

Aviel D. Rubin
ACCURATE Director
Department of Computer Science
Johns Hopkins University
rubin@cs.jhu.edu
http://www.cs.jhu.edu/~rubin/

Dan S. Wallach
ACCURATE Associate Director
Department of Computer Science
Rice University
dwallach@cs.rice.edu
http://www.cs.rice.edu/~dwallach/

Dan Boneh
Department of Computer Science
Stanford University
dabo@cs.stanford.edu
http://crypto.stanford.edu/~dabo/

Michael D. Byrne
Department of Psychology
Rice University
byrne@rice.edu
http://www.ruf.rice.edu/~byrne/

David L. Dill
Department of Computer Science
Stanford University
dill@cs.stanford.edu
http://verify.stanford.edu/dill/

Douglas W. Jones
Department of Computer Science
University of Iowa
jones@cs.uiowa.edu
http://www.cs.uiowa.edu/~jones/

Peter G. Neumann
Computer Science Laboratory
SRI International
neumann@csl.sri.com
http://www.csl.sri.com/users/neumann/neumann.html

Deirdre K. Mulligan
School of Law
University of California, Berkeley
dmulligan@law.berkeley.edu
http://www.law.berkeley.edu/faculty/profiles/facultyProfile.php?facID=1018

David A. Wagner
Department of Computer Science
University of California, Berkeley
daw@cs.berkeley.edu
http://www.cs.berkeley.edu/~daw/

Brent Waters
Computer Science Laboratory
SRI International
bwaters@csl.sri.com
http://www.csl.sri.com/users/bwaters/

Other organizations endorsing this Comment

Brennan Center for Justice at New York University School of Law
Electronic Frontier Foundation
Verified Voting Foundation

PUBLIC COMMENT OF ACCURATE
ON THE
VOTING SYSTEM TESTING & CERTIFICATION PROGRAM MANUAL

TABLE OF CONTENTS

PUBLIC COMMENT OF ACCURATE
ON THE
VOTING SYSTEM TESTING & CERTIFICATION PROGRAM MANUAL

PREFACE

A Center for Correct, Usable, Reliable, Auditable and Transparent Elections (ACCURATE), a multi-institution, interdisciplinary, academic research project funded by the National Science Foundation's (NSF) "CyberTrust Program," is pleased to provide these comments on the Voting System Testing & Certification Program Manual (the Manual) to the Election Assistance Commission (EAC). ACCURATE was established to improve election technology. ACCURATE is conducting research aimed at investigating software architecture, tamper-resistant hardware, cryptographic protocols and verification systems as applied to electronic voting systems. Additionally, ACCURATE is evaluating system usability and how public policy, in combination with technology, can better safeguard voting nationwide.

With experts in computer security, usability, and technology policy, and knowledge of election technology, procedure, law and practice, ACCURATE is uniquely positioned to provide helpful guidance to the EAC as it attempts to establish procedures for its Testing and Certification Program.

We welcome this opportunity to assist the EAC with comments from independent, academic experts who share an interest in improving election systems and their use.

INTRODUCTION

The U.S. Election Assistance Commission's release of the Voting System Testing and Certification Program (VSTCP) Manual will be a landmark in the Commission's history and in the development of electronic voting systems in the United States. As the Voluntary Voting System Guidelines (VVSG) become effective and the EAC takes charge of voting system certification at the federal level, the Manual will govern not only how manufacturers and testing labs interact with the EAC, but also how the EAC will provide information about the process to election officials and voters.

As the Manual recognizes, the EAC's role in the testing and certification process serves several important purposes grounded in the Help America Vote Act's testing and certification mandate.[1] These purposes include supporting state and local testing and certification efforts, increasing voter confidence, and increasing quality control in voting system production.[2]

The EAC, however, is not drawing on an entirely clean slate. Some of the voting systems certified under previous standards have a number of serious security, accessibility, and reliability flaws. For example, researchers have demonstrated that attackers can install a vote-stealing virus on the widely used Diebold AccuVote-TS direct recording electronic (DRE) voting system, if given a few minutes of access to a machine.[3] After the March 2004 primary election, blind voters in California stated that they were not able to vote independently and privately using Sequoia touch screen machines because of those machines' cumbersome audio interface.[4] Finally, a serious reliability issue arose in Carteret County, North Carolina, where, in November

---

[1] *See* HAVA § 231(a)(1), 42 U.S.C. § 15371(a)(1) ("The Commission shall provide for the testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories.").

[2] VSTCP Manual §§ 1.4.1-4.

[3] This attack is described by Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, Security Analysis of the Diebold AccuVote-TS Voting Machine, Sept. 13, 2006, *available at* http://itpolicy.princeton.edu/voting/ts-paper.pdf. Researchers have described several other attacks on electronic voting systems. *See, e.g.*, Craig Humphries and Craig Merchant, *Sequoia Voting Systems Vulnerability Assessment and Practical Countermeasure Development for Alameda County*, Oct. 4, 2006, *available at* http://accurate-voting.org/wp-content/uploads/2006/10/alameda_sequoia_vuln.pdf; Harri Hursti, SECURITY ALERT: Critical Security Issues with Diebold TSx, Black Box Voting, May 11, 2006, *available at* http://www.blackboxvoting.org/BBVtsxstudy.pdf; David Wagner, David Jefferson, Matt Bishop, Chris Karlof, Naveen Sastry, Security Analysis of the Diebold AccuBasic Interpreter: Report of the California Secretary of State's Voting Systems Technology Assessment Advisory Board (VSTAAB), Feb. 14, 2006, *available at* http://www.ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf; Harri Hursti, SECURITY ALERT: Critical Security Issues with Diebold Optical Scan Design, Black Box Voting, July 4, 2005, *available at* http://www.blackboxvoting.org/BBVreport.pdf.

[4] Elise Ackerman, *Blind Voters Rip E-Machines*, SAN JOSE MERCURY NEWS, May 15, 2004, *available at* www.verifiedvotingfoundation.org/article.php?id=2102.

2004, 4,400 votes were permanently lost after UniLect touch screen machines exceeded their vote storage capacity.[5] These machines did not give adequate warnings to poll workers or voters and continued to accept votes after they were full.

While these problems have been exposed, the public and election officials have gained little insight into how such flawed machines were certified in the first place. In particular, the secrecy surrounding the current certification and testing system has prevented state and local election officials, elected officials, and the public from learning about whether or how the testing and certification process failed to identify and rectify these vulnerabilities. These developments have shaken voter confidence in voting systems. The lack of accountability and transparency in the current testing and certification system has led to costly redundancies as a growing number of states have developed their own intensive testing and certification programs to supplement the federal process. Still, states take federal certification very seriously. In 2004, manufacturers were found to have fielded voting systems that were running on software that had not yet been certified in the federal process. This discovery led to considerable upheaval in California's election system, as the Secretary of State decertified Diebold machines from use in that state.[6]

The EAC faces the difficult task of supporting state and local certification efforts and increasing voter confidence with this record already in place. Although the VSTCP Manual recognizes these purposes and takes some commendable steps toward advancing them, it should do more. We note, in particular, that the Manual could more completely achieve these purposes under some of the constraints imposed on the EAC, such as the voluntary nature of the VVSG, as well as some of the choices made in the VVSG, such as the exemption of commercial off-the-shelf (COTS) components from testing.[7]

In these comments, which supplement the section-specific comments that ACCURATE has submitted through the EAC's website,[8] we highlight five principal ways in which the Manual can better serve voting system quality, state and local testing and certification, and voter confidence. In Part I, we discuss ways to support state and local testing and certification by increasing the amount of information available to election officials and the public about the

[5] Heather Havenstein, *E-Voting Woes Force New Election in N.C. County*, COMPUTERWORLD, Dec. 6, 2004, *available at* http://www.computerworld.com/governmenttopics/government/story/0,10801,98054,00.html.
[6] John Schwartz, *High-Tech Voting System Is Banned in California*, N.Y. TIMES, A5, May 1, 2004.
[7] *See* HAVA § 311, 42 U.S.C. § 15501 (making the EAC's voting system standards voluntary); VVSG, vol. I, at 4 (stating the COTS exemption).
[8] ACCURATE's section-specific comments are attached as an appendix to this document.

soundness of voting technology. We also emphasize in Part I that, while these officials and the public can provide information to the EAC after elections, they can also provide valuable information throughout the testing and certification process. The Manual should provide ways of gathering this input. In Part II, we discuss the limits in the current Manual's approach to identifying hardware and software components in fielded systems, and urge the EAC to provide additional safeguards in this area. Part III contains our suggestions for improving EAC and public oversight of voting system test laboratories by increasing the availability of information about the actual testing process. In Part IV, we discuss ways to ensure that manufacturers are responsive to the data and other needs of the Commission in its oversight and accountability functions. Finally, in Part V, we recommend that the EAC further specify the "appropriate"[9] testing methodologies to be used by VSTLs.

PART I: TIMELY PUBLICATION OF TESTING AND CERTIFICATION INFORMATION WOULD AID ELECTION OFFICIALS AND IMPROVE VOTER CONFIDENCE

The current version of the VSTCP Manual would provide some welcome insight into the testing and certification process. This insight has been almost entirely lacking until now. But when the Manual becomes effective, the EAC will publish test reports and Technical Data Packages, allowing election officials and voters much greater insight into how test labs evaluate voting systems. The EAC will also provide anomaly reports to some election officials, allowing them to learn about "irregularities" in the voting systems they field. Conversely, the Manual establishes means for the EAC to collect data from the field. All of these developments are likely to help guide state certification efforts.[10]

The Manual, however, also restricts the flow of testing- and certification-related information in ways that appear to undermine the purposes stated in the Manual. In Part I.A, we discuss four examples of restrictions on EAC publication that should be reconsidered: test plans, emergency modification waivers, anomaly reports, and official interpretations of the Manual. On the information intake side, in Part I.B, we discuss how inviting Manufacturers to provide

[9] VSTCP Manual § 4.4.1.

[10] These complementary roles of information collection and information dissemination fit not only with the Program purposes set forth in the Manual, but also with the EAC's statutory mandate to "serve as a national clearinghouse and resource for the compilation of information" for a wide range of testing and certification information. HAVA § 202, 42 U.S.C. § 15322.

information directly to the EAC poses a serious risk of undermining public confidence in the federal certification program.

A. Voters and Election Officials Will Benefit from Clearer Publication Policies

The Manual misses several opportunities to require the publication of information that governments, state and local elections officials, and the public would benefit from knowing. As ACCURATE explained in its comments on the 2005 VVSG, opening voting technology and election processes to inspection by all members of the public, particularly in the context of certification, is essential to establishing public confidence in elections.[11] In several places, the Manual fails to state a policy that is either for or against default publication of certain kinds of information. This approach is bound to create confusion and controversy over what testing and certification information the EAC will release as well as what is happening at various stages of the process. More importantly, this uncertainty is likely to delay the release of information that the public is entitled to receive. Finally, this uncertainty will hamper the flow of information within the election system, thereby impeding the feedback of field experience, standards development and certification, and voting system development and production.

Voting system standards are a linchpin in this system, yet the Manual fails to state precisely how the EAC will use information from actual election experience to shape these standards. Nor does the Manual state how often the standards will be updated, or how the EAC will go about this project. Instead, the Manual simply states that the EAC will "routinely update[]" the standards, giving no indication of what period of time is "routine."[12] The Manual should define a regular interval for voting system standards updates. This step alone would provide the public with valuable information about how to provide information that can improve the standards in general, and the testing and certification elements in particular.[13] Another broad,

---

[11] ACCURATE, Public Comment on the 2005 Voluntary Voting System Guidelines 10, *available at*.http://accurate-voting.org/accurate/docs/2005_vvsg_comment.pdf (ACCURATE VVSG Comments).

[12] VSTCP Manual § 3.2.2.1.

[13] *See* ACCURATE VVSG Comments, *supra* note 11, at 8 (advocating "[f]ormalizing and regularizing the development of the Guidelines"). Note that other areas of standards-setting that involve computerized information technology typically have a much more rapid and frequent updating of relevant standards in order to reflect the pace of innovation in information technology. While these updates are more frequent, they result in smaller changes to the standards. The EAC's voting system standards should move in this direction so that each new standard would not necessarily mean that manufacturers have to design an entirely new voting system to be compliant. For example, in avionics hardware and software, subsystems are designed knowing that they will be swapped out in the future as new, better functionality becomes available. Voting systems and the certification process could learn from

procedural topic that the Manual leaves untouched is how jurisdictions will maintain VVSG-compliant voting systems in the face of "routinely" changing guidelines, or alternatively, what significance VVSG compliance will have if standards are routinely updated yet previous standards remain in effect.[14]

In addition to providing this general guidance, there are several Manual provisions that should be enhanced or added to improve the flow of testing and certification from the EAC. Again, it is helpful to view the testing and certification process as part of a system; although the Manual outlines a linear process from VSTL testing to EAC review and certification, we emphasize how specific stages in this process should create and receive feedback from other parts of the system. For example, the experiences of voters and elections officials can inform certification or emergency modification waiver decisions that are still pending, rather than only providing a means of evaluating those decisions after they have been made.

1. Test Plans

Test plans, which provide a binding description of the tests that a VSTL will perform on a voting system, provide an appropriate starting place for this discussion. The first place that privately developed voting systems meet review by a federally regulated institution is in the VSTL, and the EAC's first substantive action under the Manual is to review the test plan for a voting system.

The Manual should provide that the EAC will publish all voting system test plans, including test plans that the Program Director rejects as unacceptable.[15] Test plans are critical documents in the testing process; they describe which components of voting system a VSTL will test and how the VSTL will conduct those tests.[16] As a result, test plans provide a crucial link between a Manufacturer's Technical Data Packages (TDP), which the Manufacturer submits to the EAC to provide the specifics of a voting system, and the test report that a VSTL submits to the EAC after it tests that voting system.[17] Under § 5.13 of the Manual, the EAC will publish redacted versions of a certified voting system's TDP and test report. Without the test plan, however, government and public overseers will have a limited ability to determine how the TDP

---

this model such that their subsystems could be updated to reflect new standards without replacing entire voting systems.

[14] This is an especially important question for the 39 states that, through their elections code or regulations, require federally certified voting systems.

[15] *See* VSTCP Manual § 4.4.2. We discuss test plans in greater detail in Part III of this document.

[16] *See* VVSG, vol. I at. A-18 (defining "test plan").

[17] See *id.* (defining "Technical Data Package") and *id*. at A-13 (defining "national certification test report").

was used to conduct tests and produce the test report. Unless the EAC supplies this link between the TDP and the test report, the value of the information in both of these types of documents will be unacceptably diminished.

2. Emergency Modification Waivers

Consistent with the Manual's stated policy of "mak[ing] the certification process as open and public as possible,"[18] the Manual should specify that the EAC will publish all information about modification waivers, regardless of whether a given waiver is granted or denied. A waiver allows a Manufacturer to modify a voting system for an election without certifying the modification and without causing the voting system to be decertified.[19] This is a major exception to the rule that "[a] Any modification to a voting system will require testing and review by the EAC."[20] Alerting elections officials and the public of how such changes are handled is essential for their roles in the election system.

Thus, the EAC should provide public notification at the very beginning—when a Manufacturer applies for an emergency modification waiver.[21] A waiver application requires only one state or local chief elections official to state that a modification is necessary to field a voting system in an upcoming election,[22] yet the voting system in question is probably being used in more than one jurisdiction. Officials in those jurisdictions have an interest in learning about whatever "emergency situation" underlies the need for a modification waiver.[23] Publishing each waiver application, including the name and title of the official who made the request, as soon as it is received would greatly help to spread this information.

The EAC also must provide public information about its action on *all* waiver applications. Currently, the Manual states only that the EAC will "issue a letter" when it grants an emergency modification waiver.[24] Thus, it is unclear whether the EAC plans to publish such letters, or otherwise provide public notification that it is allowing a voting system to be modified in the few weeks before an election. Moreover, § 3.5.7 of the Manual, which governs waiver

[18] VSTCP Manual § 1.12.
[19] *Id.* § 3.5.
[20] *Id.* § 3.4.3.
[21] *Id.* § 3.5. If, however, disclosure before an election would pose a significant risk to the security of a voting system, the Manual should establish a procedure for publishing information about the waiver application immediately after the relevant election.
[22] I*d.* § 3.5.3.2.
[23] *Id.* § 3.5.
[24] *Id.* § 3.5.5.

request denials, does not specify the form of denial, nor does it say to whom the EAC will provide notice of a denial. In both cases, as soon as the EAC has decided whether to grant or deny a waiver, it should publish a letter setting forth the grounds for that decision.

3. Anomaly Reports

Experience with voting systems in the field, as ACCURATE emphasized in its 2005 VVSG Comments, provides data that are essential to ongoing assessments of voting machine performance and the development of voting system standards.[25] Section 8.7.2 of the VSTCP Manual moves in the right direction by stating that the EAC will accept anomaly reports from "[s]tate or local election officials who have experienced voting system anomalies in their jurisdiction." Although this is a description that appears to fit a broad array of election system officials, from poll workers to chief elections officials, it excludes others who could provide useful information about voting system malfunctions. Individual voters, for example, would be a vast source of anomaly information. The task of collecting reports from any voter might appear daunting, but it is worth noting that both the Department of Justice and the nonprofit Election Protection Coalition have set up reporting systems that operate on this scale.[26]

The current version of this section also appears to rule out reports from technical experts who test fielded machines and discover flaws in accessibility, usability, reliability, and security. Reports from these experts might inform the EAC of anomalies, and allow Manufacturers and election officials to resolve them, well before an election is held. By expanding § 8.7.2, the EAC could gain access to valuable expertise and a wide range of voter experiences.

Furthermore, the EAC would better serve its testing and certification goals by publishing credible anomaly reports on its website. The VSTCP Manual, in its current form, limits distribution of credible reports to "State and local election jurisdictions who field similar systems and the Manufacturer of the voting system at issue."[27] There is little reason to restrict distribution to this group. Anomaly reports would provide useful information for jurisdictions that are considering the purchase of a voting system. Academic researchers, such as those in ACCURATE, who are working to improve the implementation and administration of voting systems would also benefit from the information in these reports. The EAC will have assessed

[25] ACCURATE VVSG Comments, *supra* note 11, at 6-8.
[26] Voters can submit input to the Department of Justice's Voting Section via: http://www.usdoj.gov/crt/voting/. The Election Protection Coalition operates the Election Incident Reporting System: http://www.866ourvote.org/.
[27] VSTCP Manual § 8.7.4.

the reports it publishes, leaving little risk that they contain inaccurate information. Once in the possession of state or local officials, the reports will likely be subject to public records act requests. It is also difficult to see how public distribution of these reports would threaten security, given the extent of distribution established in the current version. In any event, the limitation on distribution does not appear to be an effective way to mitigate any security risks in the anomaly reports.

Finally, the Manual should provide a means to protect the identity of anomaly report submitters. Although allowing anonymous submissions might hamper the EAC's efforts to substantiate reports, including the names of submitters might discourage individuals from reporting in the first place. An election official, for example, might be reluctant to report an irregularity in a system that he was responsible for administering. As a result, the quality and breadth of information that the EAC receives could suffer. Making reports confidential, or providing reporters with the option to remain confidential, would provide a workable balance between these concerns.

4. Interpretations

A final area in which the VSTCP Manual could advance the EAC's role as a source of voting system information is in its handling of Interpretations of voting standards. Currently, the VSTCP Manual allows only Manufacturers (or their agents "such as VSTLs"[28]) to request that the EAC clarify the language of the Manual in the context of a specific factual situation.[29] The need to limit requestors to parties that can present a sufficiently detailed set of facts is understandable, but the limitation in the Manual is more restrictive than necessary to address this concern. Election officials, or researchers who have obtained access to a voting system, seem well situated to provide a fact pattern to frame an Interpretation.[30]

The VSTCP Manual also prescribes significant limits on the publication of Interpretations. These limitations are detrimental to the interests of Manufacturers, officials and the public.[31] Publishing only selected Interpretations has at least two disadvantages, which a policy of publishing all Interpretations would address. First, the VSTCP Manual currently

[28] *Id.* § 9.3.1. As ACCURATE notes in the comments it submitted through the EAC's Web interface, it is inappropriate to characterize VSTLs as "agents" of Manufacturers.
[29] *Id.* § 9.1.
[30] In any event, the Manual provides a way to deal with unclear Interpretation requests: The Commission may choose to decline the request. In such cases, the EAC should publish the request and the fact that the EAC has denied it.
[31] VSTCP Manual § 9.7 ("[T]he Program Director shall select Interpretations for general publication.").

provides that the EAC will not issue Interpretations on issues that "have previously been clarified."[32] Thus, if two Manufacturers raise the same question, it is conceivable that only one of them will receive the benefit of the EAC's Interpretation. Publishing all Interpretations would eliminate this risk. Second, a policy of automatic publication would allow all election system participants to obtain a complete picture of the EAC's reading of the voting standard in question. An Interpretation allows others to understand the EAC's approach to testing and to assess more substantively how well the Testing and Certification Program is working. Published Interpretations will boost the confidence of all election system participants that the EAC's interpretations of voting standards are consistent and predictable. The selective publication model, by contrast, leaves open the question of whether bias in one direction or another influences publication decisions.

B. Limiting VVSG Interpretation Requests to Manufacturers and Allowing Manufacturers to Introduce New Facts During Appeals Undermine the Testing and Certification Process

As discussed above, increasing voter confidence requires that the EAC take in the right kinds of information, in addition to making information available. In the discussion of anomaly reports, we pointed out that the current draft of the VSTCP Manual would preclude timely reports from experts in accessibility, usability, security, and other relevant areas. Similarly, by allowing only Manufacturers and their agents to request Interpretations, the Manual creates the possibility that one Manufacturer will gain an advantage over another and that the EAC will open itself to suspicion of publication bias. Furthermore, by preventing state and local election officials—who are major purchasers of voting systems—from requesting Interpretations, the current draft will deprive these officials of a valuable means of clarifying the VVSG as they field voting systems. These examples illustrate how constraining the flow of information to the EAC in one context can have negative effects in other parts of the testing and certification system and render the EAC less transparent.

Just as importantly, however, the VSTCP Manual contains a noteworthy instance of soliciting information that is likely to create ill effects in several areas of the Testing and Certification Program. Specifically, § 6.9.3.3 would allow Manufacturers to submit materials such as "additional test data, technical analyses, and statements" in support of a request for

[32] *Id.* § 9.3.4.2.

reconsideration of a denial of certification. Similarly, § 7.7.2.3 would allow a Manufacturer to "provide relevant facts (such as technical information, testing data, or statements)" to support an appeal of denial of certification.

These provisions have a pernicious effect on at least two other parts of the testing and certification system. First, they diminish the standing of VSTLs as the "independent" laboratories that HAVA establishes as the workhorses of the testing and certification process. VSTLs, of course, must be evaluated by NIST and accredited by the EAC; and, under the VSTCP Manual, they must submit their test plans and test reports to the EAC. Put simply, the EAC knows what the VSTLs did to test a voting system. There are no such safeguards for the Manufacturer-controlled tests that § 6.9.3.3 and § 7.7.2.3 would allow, yet the VSTCP Manual apparently would put these submissions on equal footing with results from a VSTL. A VSTL's incentives to be impartial could be severely undermined, if the laboratory knows that a Manufacturer ultimately has the option of submitting unchallenged facts to the record.

The second negative effect of this section concerns confidence in the EAC itself. The VSTCP Manual does not state a policy concerning publishing submissions for systems that are denied certification.[33] In fact, the Manual in its present form does not even provide explicitly for the publication of requests for reconsideration.[34] Thus, it is possible that the EAC will deny certification of a voting system on the basis of documents and information provided by a VSTL, then reverse this decision on the basis of "relevant facts" quite possibly created *after* the Initial Decision denying certification and supplied by the Manufacturer; and the EAC expresses no commitment to making these facts public.[35] While reconsideration and appeals are standard procedural options offered by many kinds of adjudicative bodies, we can think of no tribunal that allows a party seeking reconsideration or reversal of a decision free rein to enter new facts into the record. The EAC should publish requests reconsideration as soon as it receives them, and it should not allow Manufacturers seeking reconsideration to submit new evidence.

PART II: RECOGNIZE THE LIMITS OF HARDWARE AND SOFTWARE IDENTIFICATION

[33] This is in stark contrast to grants of certification, in which case the EAC will publish the VSTL's test report, among other documents. VSTCP Manual § 5.13.

[34] *See* VSTCP Manual § 6.9.2 ("The Decision Authority shall *acknowledge* receipt of the Manufacturer's request for reconsideration.") (emphasis added).

[35] We do not see a plausible reading of § 5.13, which governs publication of information when certification is granted outright, that would cover certification after reconsideration under § 6 of the Manual.

In the context of voting system verification, the VSTCP Manual takes a step toward providing federal, state, and local elections officials with a means of testing whether their fielded voting systems are the same systems that were certified: Section 5.8 of the VSTCP Manual requires Manufacturers to provide "system identification tools" that "verify that the equipment used in elections is unmodified from its certified version." While elections officials will very likely appreciate the EAC's role in making these informational tools available, the VSTCP Manual could do more to ensure that these tools produce trustworthy information.

Verifying software in this sense—checking whether the software on a fielded voting system is the same as the software that was certified and establishing that a system does not contain any uncertified software—remains an open problem and active research frontier in computer science.[36] Both elements of this kind of identification are important but require careful implementation. As explained below, unless it is done with great care, the process of checking whether installed software matches the certified versions opens up a new vector for attack where a legitimate system could be replaced with a malicious one. Conversely, it is critical to check a fielded system for files that are uncertified and should not be present. The introduction of malicious executable code outside of certified software was the basis for the attack recently reported by researchers at Princeton University, yet the software identification scheme proposed in the Manual would not detect such files.[37] We do not fault the EAC for failing to provide a solution, but we do point out several steps that the EAC could take, through the VSTCP Manual, to improve the quality of information from system identification tools.

First, the VSTCP Manual must require that standardized system identification tools receive independent review and follow a trusted path for distribution. Independent review is necessary to detect malicious tools.[38] A system verification tool that has not been reviewed could easily be designed to misreport verification details or even modify the software on the fielded system. That is, this section, in its current form, could actually facilitate attacks.

---

[36] We believe that the Manual's use of the term "verification" is at odds with its generally accepted uses in computer science. For both hardware and software, verification typically refers to logical proofs of the correctness of a design. This term can also refer to an industry standard for simulation and testing. What the VSTCP Manual specifies is better described as identifying software and hardware against the components that were certified.

[37] *See* Princeton Report at 5, 12-15 (describing how a vote stealing virus was introduced into a Diebold AccuVote TS).

[38] Ideally, these tools would be developed independently of a Manufacturer. Because these tools require detailed knowledge of the voting system, however, independent development might not be workable under the current regulatory framework. We present independent review as the next-best alternative.

Independent review of the tools would reduce the likelihood of such attacks. Similarly, a trusted distribution path—for example, having the EAC cryptographically sign and distribute identification software—would provide stronger authentication of the software that is used in the field. To enforce this distribution path, the Manual should recommend to election jurisdictions that the signatures of all system identification tools are compared with the independently reviewed version before the tools are installed or used on a fielded voting system.

Second, the software-specific portion of this section must state more stringent requirements for the criteria used to conclude that the software on a fielded system is the certified software. This subsection simply states that "digital signatures" must be used to identify "application files" and "executables"; "signatures" are required for "all nonvolatile files that the application files access during their operation."[39] Digital signatures vary widely in the amount of security they provide; some are known to be susceptible to attacks that can be carried out on modern commodity hardware.[40] Nonetheless, a Manufacturer could comply with the current requirement by using any digital signature. The danger here is real: Systems currently in use have made inappropriate use of cryptographic tools. The Diebold TS and TSx, for example, used widely known cryptographic key and thus introduced a serious flaw into its digital signature scheme. Similarly, Sequoia AVC Edge systems all use the same key for their digital signatures, increasing the likelihood that the key will be discovered and lead to the compromise of these machines.[41] Requiring compliance with Federal Information Processing Standard 140 (FIPS 140) would address these problems and provide a convenient way for the EAC to keep its cryptography-related requirements up-to-date.[42] While the EAC might not wish to specify which digital signature algorithms must be used in system identification tools, it must require these tools to use algorithms that are widely accepted by cryptographic experts to be secure and must provide a means to update these algorithms if they are later found to have vulnerabilities.

Third, the Manual provides very little guidance for the hardware configuration that many electronic voting systems use. Most systems do not boot from CDs, and it is unclear what the

---

[39] VSTCP Manual § 5.8.2.

[40] For example, digital signature algorithms that rely on the DES cipher fit this description. DES has been known to be vulnerable since 1998. *See:* John Gilmore, CRACKING DES: SECRETS OF ENCRYPTION RESEARCH, WIRETAP POLITICS AND CHIP DESIGN, 1998, O'Reilly, ISBN 1-56592-520-3.

[41] *See* Alameda Report on Sequoia, supra note 3, at iii.

[42] The current version of FIPS-140, which is published by NIST, is available at http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf. A general description of FIPS 140 is at FIPS 140, http://en.wikipedia.org/w/index.php?title=FIPS_140&oldid=78729144 (last visited October 30, 2006).

criteria are for determining whether another medium is "similar."[43] For boot devices other than a "self-booting CD or similar device[s]," the Manual simply declares that "a procedure must be provided" for "identification and verification."[44] The Manual must provide more specific requirements for verifying the software on such systems. For example, the Manual should require (1) that the tools be produced by a person who has no financial or other interest in a Manufacturer, (2) that a VSTL test the identification tools, (3) that the media containing the tools be handled through a chain of custody that minimizes the risk that the tools themselves will be corrupted, and (4) that the source code for software verification tools be published.

In the future, the EAC should consider going beyond checking cryptographically secure checksums. A promising scheme has been developed for checking the ROM contents of a casino game.[45] Although adapting this method for voting systems would require additional time and research, as well as certain requirements for voting system hardware, it would provide a more stringent and flexible method for checking voting system software. An alternative approach would be to incorporate hardware- and software-based security components that are now reaching the mass market. The Trusted Computing Group (TCG), for example, is developing a system of hardware modules that can add some assurance that a machine has booted into a specific configuration.[46] Microsoft's next-generation operating system interacts with TCG-based hardware to provide cryptographically sealed storage. Still, the TCG approach has its limitations, not only because the technology itself is new, but also because it is not designed to prevent attacks—which have been demonstrated in existing machines[47]—arising from code that is injected after a machine is booted.

---

[43] Possibilities include removable, read-only, etc. To the extent that the read-only property is the basis for similarity, note that the contents of some kinds of storage widely thought to be "write-once" can be manipulated. For example, at least one person has successfully modified the programmable read-only memory (PROM) chips in slot machines in Nevada to pay out when a player used a specific series of bets. Sean Whaley, *Former Gaming Official Sent to Jail for Slot Scam*, LAS VEGAS REVIEW-JOURNAL, 1A, Jan. 10, 1998.

[44] VSTCP Manual § 5.8.2.

[45] *See* U.S. Patent No. 6,149,522 (issued Nov. 21, 2000), http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&co1=AND&d=PTXT&s1=6,149,522.PN.&OS=PN/6,149,522&RS=PN/6,149,522.

[46] For a thorough summary of TCG hardware, see generally John Marchesini, Sean Smith, Omen Wild, and Rich MacDonald, *Experimenting with TCPA/TCG Hardware, Or: How I Learned to Stop Worrying and Love The Bear*, Dartmouth Computer Science Technical Report TR2003-476, Dec. 15, 2003, *at* http://www.cs.dartmouth.edu/%7Esws/papers/mswm03.pdf.

[47] See the studies cited above in footnote 3.

The hardware checking provision[48] is superficial and unlikely to provide much assurance that a given voting machine contains certified hardware. Again, verifying the authenticity of a voting machine in the field is simply an unsolved problem; it is very difficult to provide rigorous requirements that are still practical for election environments. Nonetheless, it is worth pointing out some of the limitations on the Manual's approach of relying on "detailed photographs" as the basis for checking voting system hardware in the field. If the circuitry contains programmable array logic or field programmable gate array components, these components could look identical to a photograph while containing entirely different functionality.[49] Thus, the Manual's photo-identification approach might provide a false sense of security against hardware containing unauthorized modifications. Moreover, an attacker might be able to replace hardware with apparently identical components if given just a few minutes of access to a voting machine. More carefully checking these hardware components would involve removing them from the fielded voting system, plugging them into an external reader, and comparing the logic they contain with the logic programmed on the certified components. This level of checking is probably not practical on a wide scale.

PART III: ENHANCE CONFIDENCE IN TESTING VOTING SYSTEM TEST LABORATORIES (VSTLS) BY INCREASING THEIR DIRECT ACCOUNTABILITY TO THE EAC

In the previous two Parts of these comments, we have discussed how changes to the VSTCP Manual would support state certification efforts and increase voter confidence by publishing more testing- and certification-related information. We have also discussed how the Manual must take a more cautious approach to mandating the use of tools that purport to provide information about the software that is installed on fielded voting systems. In this Part, we discuss ways in which the Manual can better ensure the quality of information that flows from a key player in the testing and certification program: the VSTLs.

Generally speaking, the VSTCP Manual should promote VSTL objectivity and neutrality. In its current version, the Manual would replicate features of the previous system's ITA-Manufacturer relationship that we have criticized in the past. For example, the Manual does not

[48] VSTCP Manual § 5.8.1.

[49] EPROM and EEPROM components present similar difficulties. The extent to which modern systems depend on programmable hardware raises the question of whether the COTS exemption should apply to them, and if so, whether these components should be removed from the exemption.

change the fact that Manufacturers select and pay their own test labs.[50] This arrangement allows a Manufacturer to choose the lab that it believes will be most favorable and, if it is dissatisfied, to choose another. As a result, the Manual will not increase the minimal incentives that test labs currently have to conduct stringent tests.[51] Moreover, a test lab recently stated in a written submission to the EAC that it "view[s] the relationship between an independent testing laboratory and it's [sic] clients as similar to that between lawyer and client or between doctor and patient."[52] Although federal law does not recognize a privilege against the compelled disclosure of communications between a Manufacturer and a VSTL, as it does with attorney-client communications, this statement illustrates the strong sense of duty that at least one test lab feels to keep secret information about its clients. This sense of duty is unlikely to change unless the EAC limits direct relationships between VSTLs and Manufacturers,[53]

Although publicly releasing VSTL test reports for voting systems that obtain certification is an important step that will provide election system participants with much-needed information about testing and certification,[54] subject to redaction, the Manual should expose information that is gathered further back in the process. We note three specific provisions of the Manual that should be changed to provide this insight. First, the VSTCP Manual should prohibit VSTLs from sending test plans to, or discussing them with, Manufacturers before the laboratories send the test plans to the EAC. Currently, the Manual makes no statement about the extent to which communications between a Manufacturer and the VSTL that it has chosen are permissible, leaving open the possibility that these two parties will negotiate a test plan. Although test plan review and approval by the EAC will assure that test plans meet voting system guidelines, the

[50] *See* ACCURATE VVSG Comments, *supra* note 11, at 4.
[51] As we point out in the Introduction, several systems that were tested and subsequently certified have had severe security, usability, and accessibility flaws.
[52] Wyle Laboratories, Inc., Written Statement for EAC Public Meeting and Hearing, Oct. 26, 2006, *at* http://www.eac.gov/docs/Voting%20Systems%20Briefing%20-%20Frank%20Padilla%2010-18-06%20Final.pdf.
[53] We are aware that an obvious way to reform direct payment of VSTLs by Manufacturers—namely, requiring the EAC to select and pay VSTLs—might require additional administrative structure or authorization from Congress. For this reasons given in this Part, however, pursuing such a long-term solution would be extremely valuable in improving oversight of the Testing and Certification Process.
[54] *See* VSTCP Manual § 5.13. As we argue in Part I, the EAC should publish the same materials for voting systems that are denied certification. We also argue that the EAC should publish test plans for every voting system that enters the testing and certification process, irrespective of whether it is granted certification.

testing and certification system would benefit from requiring VSTLs to develop their own interpretations of those guidelines.[55]

For similar reasons, the VSTCP Manual should require VSTLs to report changes in an approved test plan, test failures, and test anomalies directly to the EAC. The current version of the Manual makes Manufacturers responsible for ensuring that VSTLs make these reports.[56]

Finally, the VSTCP Manual should directly require VSTLs to send test reports to the EAC, rather than routing this requirement through Manufacturers.[57]

PART IV: EMPHASIZE MANUFACTURERS' DUTY TO COOPERATE WITH THE EAC

Manufacturers are crucial sources of information for the EAC. In this Part, we discuss ways in which the VSTCP Manual can promote their cooperation with the EAC. Deregistration is the primary disciplinary mechanism in the Manual. A Manufacturer must register with the EAC before it may participate in the Testing and Certification Program, and deregistration can lead decertification of a Manufacturer's voting systems.[58] Decertification, as the Manual notes, is "an important part of the Certification Program" but is also a "serious matter" that "will significantly affect" the public, governments, elections official, and Manufacturers.[59] Thus, many groups share an interest in preventing problems with a voting system from escalating to decertification.

Investigating possible violations of voting system standards or of the VSTCP Manual's procedures, however, will require significant time from the EAC; and the EAC has a strong interest in concluding these investigations before an election is imminent. Because Manufacturers are likely to be the single greatest source of information in these investigations, securing their full cooperation is critical to the EAC's investigative and oversight roles.

---

[55] As we point out in Part I, allowing VSTLs to request Interpretations on their own behalf would also help to achieve this goal.
[56] VSTCP Manual § 4.5.
[57] *See* id. § 4.6 ("Manufacturers shall have their identified test lab submit test reports directly to the EAC."). The EAC should require test reports in all cases, not only when a voting system "has been successfully tested." *Id.* § 4.6; *see also* Part I of these Comments.
[58] VSTCP Manual §§ 2.2 (no certification without registration); 2.6 (stating that failure to remedy suspended registration can lead to decertification); and 7.2 (stating that voting systems "shall be decertified" if "the Manufacturer has . . . failed to follow the procedures outlined in this Manual," among other reasons).
[59] *Id.* § 7.1.

The current draft of the VSTCP Manual establishes that the EAC may suspend a Manufacturer for any violation of Testing and Certification Program procedure,[60] including refusal to "cooperate" with the Commission.[61] We point to two ways in which changes to the current draft of the VSTCP Manual would advance the EAC's interest in timely and thorough investigations. First, the Manual should make clear that a Manufacturer's failure to comply within a specified time with any method of investigation will initiate action to suspend the Manufacturer. The current draft of the Manual only draws this connection with respect to written interrogatories.[62]

Second, given the strong public interest in the outcome of the EAC's investigative work,[63] it is appropriate to make public, at some point, a Manufacturer's refusal to cooperate with an investigation. For example, the Manual should specify that the EAC will publish notice of any Notice of Non-Compliance it issues to a Manufacturer.[64] In addition, the Manual should require public notice of actual suspensions of registration; the current draft does not state a clear policy on this point.[65] In summary, increased public disclosure of EAC actions regarding Manufacturer suspension will likely help the EAC obtain the information that it needs to conduct investigations and strengthen its administration of the Testing and Certification Program.

A final issue that concerns Manufacturer cooperation with the EAC is the Manual's trade secret and confidentiality policy.[66] To be sure, trade secrets and confidential commercial information that Manufacturers submit to the EAC are protected from disclosure under the Freedom of Information Act (FOIA), and the Manual hews closely to the interpretations of those terms given in the FOIA case law.[67] The Manual wisely places the burden on Manufacturers to identify, specifically and at the time of submission, which information they consider trade secret

---

[60] *Id.* § 2.6.1.
[61] *Id.* § 2.6.1.3.
[62] *Id.* § 7.4.5.5.4.
[63] *See id.* § 7.4.5 ("Because voting systems play a vital role in our democratic process, investigations shall be conducted impartially, diligently, promptly, and confidentially. Investigators shall use techniques to gather necessary information that meet these requirements.").
[64] *Id.* § 2.6.1.3.
[65] *Id.* § 2.6.1.4.
[66] *See generally id.* § 10.
[67] 5 U.S.C. § 552(b)(4). The leading case governing exemption from FOIA of confidential commercial information that the government requires to be submitted is *National Parks & Conservation Ass'n v. Morton*, 498 F.2d 765 (D.C. Cir. 1974). Exemption from FOIA of information that is voluntarily submitted is governed under a different standard. *See* Critical Mass Energy Project v. NRC, 975 F.2d 871, 877 (D.C. Cir. 1992) (en banc). A helpful oversight of the trade secrets and confidential information exemption is available from the U.S. Department of Justice, Freedom of Information Act Guide, Exemption 4, May 2004, *at* http://www.usdoj.gov/oip/exemption4.htm.

or confidential.[68] The Manual also asserts that the EAC is "ultimately responsible" for determining which information may not be disclosed to the public.[69]

In other ways, however, the Manual presents a distorted picture of its responsibilities relating to FOIA. For example, § 10.6.2.2 permits a Manufacturer to "provide input" to the EAC regarding any request for potentially protected records submitted by the Manufacturer. This is consistent with current federal policy, but the Manual fails to mention that that policy also requires the EAC to notify the information requester and allow it an opportunity to comment.[70] The Manual must correct this deficiency. In addition, the Manual should provide greater detail about the proceedings that the EAC will hold, and the record that it will assemble, to determine whether requested information is exempt from disclosure. These details are necessary to provide guidance to requesters and Manufacturers, to establish orderly handling of requests within the EAC, and to provide federal courts with a useful record in the event a request leads to litigation. Manufacturers have repeatedly taken the position that a broad array of information about their systems is either a trade secret or is considered confidential.[71] Since the EAC will be handling much more of this information that it has in the past, a thorough plan for handling objections of requesters and submitters to the EAC's disclosure decisions will be essential. Finally, the Manual must specify procedures that take into account the strict timeframe that FOIA will impose on the EAC.[72]

PART V: REQUIRE DISCIPLINE-SPECIFIC, STATE-OF-THE-ART TESTING METHODOLOGIES

Section 4.4.1 of the Manual requires that VSTLs "develop test plans that use appropriate test protocols, standards, or test suites." The Manual, however, does not define which testing

[68] VSTCP Manual § 10.7.
[69] VSTCP Manual § 10.6.
[70] *See* Executive Order 12,600, Predisclosure Notification Procedures for Confidential Commercial Information, June 25, 1987, available at http://www.cftc.gov/foia/foieo12600.htm. In particular, see § 1, which requires notification of the information submitter, and § 9, which requires notification of the information requester in response.
[71] For example, Diebold Election Systems, Inc. issued a letter to the Ohio Board of Elections stating that it would "seek all legal and equitable remedies available to it" if the Board released any information that Diebold considered trade secret or confidential. Letter from Diebold Election Systems, Inc. re Diebold's Position on Releasable Materials for Open Records Requests, Jan. 13, 2006 (on file with authors).
[72] Specifically, an agency has 20 days to decide whether requested information otherwise subject to FOIA is exempt as a trade secret or confidential commercial information. 5 U.S.C. § 552(a)(6)(A)(i). A requester who does not receive a response within this time may file suit in the appropriate federal district court to compel a response. § 552(a)(6)(C)(i).

methods (by which we mean test protocols, standards, and test suites) are "appropriate"; nor does the Manual provide criteria for deciding whether a given method is "appropriate."[73] Thus, the Manual misses an opportunity to provide VSTLs with guidance and to inform the public about the standards to which the EAC is holding VSTLs. Providing additional guidance about testing methods could also promote the EAC's goal of increasing voting system quality control.[74] The EAC could advance all of these purposes by requiring that VSTLs use discipline-specific testing methods that represent the state-of-the-art in the respective discipline for measuring the performance of voting systems.

In ACCURATE's comments on the VVSG, we noted that evaluation methodologies should be tailored for each domain that the requirements cover: "The Guidelines must move away from a simple reliance on functional testing and embrace a more sophisticated and nuanced evaluation regime that is primarily designed to assess whether a systems' performance meets established goals."[75] In the area of security testing, these methods would include threat models and threat assessment, code review, and red-team testing.[76] Another important testing discipline, usability, might include user testing using a significantly sized, representative sample of actual voters.

[73] The Manual only defines the consequence of submitting a test plan that is not found to be appropriate. According to § 4.4.4.2, "[i]f a plan is not accepted, the Program Director will return the submission to the Manufacturer's identified laboratory for additional action."
[74] VSTCP Manual § 1.4.3.
[75] ACCURATE VVSG Comments, *supra* note 11, at 6.
[76] *See id.* at 13-18.

CONCLUSION

The current draft of the VSTCP Manual would provide election officials and voters with significant amounts of testing- and certification-related information that has, until now, been difficult or impossible to obtain. The Manual, however, should go further to ensure that the EAC will publish all relevant information by default and in a timely fashion. Clear policies in favor of publication will not only serve these groups but also will improve the EAC's ability to oversee the testing and certification process. Finally, the Manual should more explicitly recognize the limitations on its proposed means for identifying voting system components in fielded systems. With these changes, the VSTCP Manual will more likely increase voter confidence and more fully support state and local election officials.

Submitted on behalf of ACCURATE and listed affiliates by:
Aaron Burstein, ACCURATE Research Fellow, Samuelson Law, Technology & Public Policy Clinic and Berkeley Center for Law and Technology, Boalt Hall School of Law, University of California, Berkeley
Joseph Lorenzo Hall, Ph.D. Student, School of Information, University of California, Berkeley
Deirdre K. Mulligan, Director, Samuelson Law, Technology & Public Policy Clinic, Boalt Hall School of Law, University of California, Berkeley

APPENDIX: Section-Specific Comments That Were Submitted Through the EAC's Web Interface

Section	Comments
§ 1: INTRODUCTION	
1.5.1.8	The EAC should accept requests for Interpretations from persons other than VSTLs and Manufacturers. We provide more specific comments under § 9.3.1.
1.5.2	Clarify the circumstances under which "immediate implementation" of a change in policy is necessary. The policy memorandum announcing such changes should be published at the same time the memorandum is issued to Manufacturers.
1.6.1.2	EAC certification is frequently a necessary, but not sufficient, condition for state certification. This section, and the Manual as a whole, should recognize the extent of state-level testing and should strive to support state and local officials' testing efforts by making available as much information from the federal testing process as possible.
1.6.2.3	Strengthen the requirements for EAC technical experts. Publish the generally applicable qualifications and job descriptions for these positions.
1.12	It should be made explicit in this section that the Commission will redact information that is exempt from release under FOIA, rather than withhold entire documents that contain FOIA-exempt information.
1.13	Definition of "installation disk": A more general term – perhaps "installation device" – should be used. Many kinds of devices, including electronic voting systems, use devices other than disks to install software. For example, some electronic voting systems use flash memory cards and PCMCIA cards to install software.
1.13	Definition of "voting system": This definition should be harmonized with the definition of "voting system" in the VVSG. Notably, the VVSG definition does not include equipment that "connect[s] the voting system to the voter registration system," as the TCP Manual does. Conversely, the TCP Manual's definition lacks many of the details found in the VVSG's definition. To provide clarity for voters, elections officials, and manufacturers, these definitions must be reconciled by either amending the VVSG Glossary or by using the VVSG definition in the VSTCP Manual.
§ 2: MANUFACTURER REGISTRATION	
2.3.1.1.4	Manufacturers to which this section applied should be required to provide all business affiliations of their directors.

Section	Comments
2.3.1.1.5	Manufacturers to which this section applies should be required to provide all business affiliations of their partners.
2.3.1.1.6	Clarify "controlling ownership interest." In the case of a corporation, control is typically defined by ownership of a certain percentage of securities or the power to designate a certain percentage of directors. In the case a partnership or other unincorporated entity, control is typically defined as the right to a certain percentage of the entity's profits or to a certain percentage of assets upon the entity's dissolution. *See* 16 C.F.R. § 801.1(b).
2.3.2.2	The requirement of affixing a permanent certification label conflicts with the Manual in two ways. First, it generally runs against the Manual's provision for the decertification of a voting system. Second, if a voting system is decertified, its Manufacturer may not represent the machine as certified. Instead of requiring permanent certification labels, the EAC should maintain on its public Web site an up-to-date list of all certified (as provided in § 5.13) and decertified voting systems. For each decertified voting system, this list should include the date of and reasons for decertification.
2.3.2.4 2.3.2.6	The Manual should be more specific about what constitutes vendor cooperation as well as what measures it will take to ensure cooperation from Manufacturers. In particular, the EAC should move to suspend the registration of a Manufacturer that fails to cooperate with the Commission.
2.3.2.5	Although inspecting a facility may provide a snapshot of quality control practices at a manufacturing facility, that snapshot is limited. Therefore, it is important to include within this section an agreement to allow EAC officials to inspect any logs, manuals, and other documents or materials it deems relevant relating to quality control.
2.3.2.7	This section should require a Manufacturer to disclose all known malfunctions of a voting system for which the Manufacturer seeks certification. This could be accomplished by rewriting the first sentence of this section as: "Report to the Program Director any known malfunction of a voting system holding or seeking an EAC Certification." In addition, this section's definition of "malfunction" should be reconsidered. It is difficult, in practice, to determine where operator error ends and machine error begins. For example, in a recent trial of the Diebold electronic poll book in Maryland it was revealed that using the poll book's touch screen, rather than an attached mouse, would cause the poll book to crash. It is unclear how to classify this event under the current language of the Manual.

Section	Comments
2.5	The EAC should require strong passwords and implement password expiration to help reduce the risk that manufacturer passwords will be compromised.
§ 3: WHEN VOTING SYSTEMS MUST BE SUBMITTED FOR TESTING AND CERTIFICATION	
3.2.2.1	This section should clarify the EAC's approach to updating its standards, including a statement of what period of time is "routine" and a commitment that the EAC will propose changes to the standards in a manner that allows a full opportunity for public comment.
3.2.2.2.2	Manufacturers should be allowed to submit voting systems for testing under a standard as soon as that standard is finalized, rather than having to wait until the standard's start date. For example, the 2005 VVSG were finalized last year but are not effective until December 2007. The current version of this section will not only delay the effectiveness of standard for two years but also removes an incentive that Manufacturers would otherwise have to compete on the basis of VVSG compliance.
3.2.2.4	This section appears to allow technology that was not anticipated in the VVSG to be added to a voting system, provided only that the new system pass integration testing; this technology does not have to pass more stringent new system testing. This section should require, at minimum, that the Manufacturer petition the TGDC for permission to add the component to the system in question.
3.4.3	This section should also require testing and review for modifications of a voting system's documentation.
3.5.2	This section should clarify that a Manufacturer must meet all requirements in §§ 3.5.2.1-8 to qualify for a waiver; replace the periods at the end of §§ 3.5.2.1-7 and add "and" to the end of § 3.5.2.7.
3.5.2.7	The Manual should provide for better oversight for testing by the Manufacturer. At minimum, the Manual should provide that the chief state or local election official who affirms the need for the emergency modification waiver (as provided under § 3.5.3.2) may supervise the Manufacturer's testing. Alternatively, the Manual could require the Manufacturer to submit the modification to a VSTL, which would complete testing to the extent possible. Note that § 3.5.3.5 envisions that "a laboratory" will be able to conduct some testing of a modification.
3.5.3	State that all requests for waivers, including all supporting documentation, will be made publicly available by the EAC as soon as practical, and in no event later than the EAC grants or

Section	Comments
	denies the waiver request.
3.5.3.1	Require the Manufacturer to sign the statement described by this section. Also, require the Manufacturer to state when it learned of the need for the modification and to include documentary evidence that supports this statement.
3.5.3.6.3	Require the chief state or local election official who supported the modification waiver (see § 3.5.3.2) to sign the report. In addition, require that this report identify and describe any usability, accessibility, or other kinds of failures not included in the current version of this section that were encountered in the election. Finally, require the Manufacturer to identify and describe publicly reported failures of the voting system that fall into these five categories.
3.5.5	State that the EAC will publish any letter granting a modification waiver on the same day that the letter is issued.
3.5.6	Include a cross-reference to § 7.2, which provides for the decertification of a system that is modified without following the requirements of the TCP Manual.
3.5.7	State that the EAC will publish its decision to deny a modification waiver, and the reasons that support the denial, on the same day that the decision to deny is made.
§ 4: CERTIFICATION TESTING AND REVIEW	
4.2	Item (2) should read: "submitted an EAC-approved test plan created by an accredited VSTL."
4.3.1.6.1	Clarify which parts of a voting system are "components."
4.3.1.6.2	Clarify which parts of a voting system are "components."
4.3.2.3	Include the OpenOffice Open Document Formats (ODF) and Rich Text Format (RTF) in the list of acceptable electronic formats.
4.3.3	Incorporate by reference the VVSG definition of Technical Data Package.
4.4	To ensure the independence of VSTLs, Manufacturers should have limited opportunity to influence test plans; this section should require VSTLs to refrain from sending a test plan to the Manufacturer until the VSTL has sent the plan to the EAC for review.
4.4.1	Whether in this section or elsewhere, the Manual should define what constitutes "appropriate test protocols, standards, or test suites." We suggest that, for each domain of the requirements in the standards, the laboratory shall use domain-specific evaluation methodologies that are state-of-the-art for that domain. For example, security testing shall include an open-ended component such as red-team testing; usability evaluation shall include user testing using a significant, representative sample of real voters.

Section	Comments
4.4.2	All submitted test plans should be made public, regardless of whether they are approved. The VSTCP Manual requires VSTL reports and Technical Data Packages (TDP) to be made public, in redacted form. However, that material is of little utility without knowing how the TDP was used to produce the VSTL report. The missing link in this process is the VSTL's test plan.
4.4.2.3	This section should specify and define three types of tests for modifications to previously certified systems: delta-testing, system integration testing and regression testing. Delta-testing is testing the modification itself. System integration testing is testing the modification in the context of the larger system, similar to but more limited than testing that is conducted to certify a new system. Regression testing is testing that attempts to discover if the modification may have introduced problems in other components of the system.
4.5	VSTLs should be made directly responsible for reporting, instead of vendors "ensur[ing] that VSTLs" report, (1) changes to a voting system or test plan and (2) test failures or anomalies to the EAC.
4.6	This section should forbid VSTLs from sending test reports to the Manufacturer before the VSTLs sends the report to the EAC. Also, this section should directly regulate VSTLs by stating, in the first sentence, "VSTLs shall submit test reports directly to the EAC." Finally, the EAC should require submission of test reports in all cases, not only when "the voting system has been successfully tested."
§ 5: GRANT OF CERTIFICATION	
5.5	Specify that a trusted build is for a specific target platform – the voting system with a specific set of hardware, software and firmware – rather than "the computer."
5.5.1.1	Re-number as 5.5.1.
5.5.1.2	Re-number as 5.5.2.
5.5.1.3	Re-number as 5.5.3.
5.5.1.4	Re-number as 5.5.4.
5.6	As we noted in a comment on § 1.13's definition of "installation disk," some voting systems use devices other than disks to install files and software. This section should refer to an "installation device" or some other term that is sufficiently general to cover the full range of devices used to install software on currently used voting systems.
5.6.1.1	Include a more specific instruction to "completely erase" the build environment. For example, ". . . the build environment shall be completely erased by the VSTL by overwriting all usable space with random data . . ."

Section	Comments
5.6.1.3	Require VSTLs to use a hash algorithm and an encryption algorithm that comply with Federal Information Processing Standard 140 (FIPS 140), which is published by NIST.
5.8	Requiring Manufacturers to provide "system identification tools" will do little to assure elections officials that a fielded system is unmodified from a certified system. At minimum, the Commission should require any software system identification tool to be independently reviewed and its source code published. The EAC should also serve as the distributor of these tools; it should provide cryptographically signed software directly to jurisdictions, rather than allowing Manufacturers to distribute the tools. Finally, the tools should be required to check their signatures with a trusted third party, such as the EAC, before they are installed or used on a voting system. Our narrative document contains an extensive discussion of this topic.
5.8.1	This section's reliance on photograph-based identification of hardware provides only a minimally meaningful check of fielded voting system hardware. This method could easily fail to identify modified hardware components. We discuss this section extensively in our narrative comments.
5.8.2	This section must require system verification tools to use digital signature algorithms that comply with FIPS 140. This section must provide specific criteria for determining whether a boot device is "similar" to a self-booting CD. This section must specify a protocol the identification and verification of software that is being used on a voting system that does not boot from a device similar to a self-booting CD. This section should also require a system identification tool to look for files that should not be present on a fielded system, based on the file map specified in the current version of this section. Furthermore, the tool should enumerate all volatile files and sign everything else on the system. Finally, this section should specify that the source code for software identification tools be made publicly available. In our narrative document we discuss in depth the difficulties of this section's current proposed approach.
5.13	This section should include a cross-reference to § 10.7, which sets forth the procedures that Manufacturers must follow to designate information as confidential. In addition, the EAC should commit, in this section, to publishing the redacted versions of all materials, including the test report, rather than withholding entire documents that contain trade secrets or commercial confidential information. Finally, this section should clearly define the "supporting test report" as being the VSTL's test report.
5.14	This prohibition is appropriate but lacks a specifically stated consequence; the EAC should move to deregister a Manufacturer

Section	Comments
	that violates this section.
5.15.3 5.15.4	As we noted in our comment to § 2.3.2.2, affixing a permanent mark of certification to a voting system creates the potential for confusion when a system is decertified. A better approach would be to maintain, along with the list of certified voting systems (see § 5.13), a list of decertified systems, including the date of and reasons for decertification.
§ 6: DENIAL OF CERTIFICATION	
6.9.2	This section should require the publication of all requests for reconsideration; the current § 6.9.2 only provides for acknowledgement of requests.
6.9.3.3	This section should be stricken. Allowing Manufacturers to submit "[o]ther written materials created to provide relevant facts" would undermine the position of the VSTL's report, which should be neutral and factual. By contrast, documents created by the Manufacturer after an Initial Decision to deny certification are likely to advocate reaching the opposite conclusion and possibly introduce new material that was unavailable to the VSTL during evaluation. This could increase the chances of "factual disputes," which are taken to be minimal in § 6.11.2.3. This section would require VSTLs to anticipate rebuttals from Manufacturers, a consideration that could subtly warp the quality and presentation of VSTL test reports. It is also highly likely that Manufacturers would claim trade secret or confidentiality protection in the documents submitted under this section. To the extent that the EAC relies on non-public documents created by Manufacturers during reconsideration, the EAC is likely to raise doubts about the reconsideration process.
6.10	The Agency Decision should be published on the EAC's website as soon as it is issued.
6.11	Requests for appeal of an Agency Decision denying certification should be published on the EAC's Web site upon receipt.
6.11.2.3	This section should eliminate its dependence on the flawed evidentiary model of § 6.9.3.3. As we state in our comments to § 6.9.3.3, a Manufacturer should not be permitted to introduce new facts into the record. Please see our comments on that section in our narrative comments. The facts found by the Decision Authority should be given greater deference than provided in the current version of § 6.11.2.3. In particular, the Appeal Authority should uphold the factual findings of the Decision Authority unless the record would compel a

Section	Comments
	reasonable fact finder to find otherwise.
6.12	All Decisions on Appeal should be published on the EAC's Web site at the same time they are provided to the Manufacturer.
§ 7: DECERTIFICATION	
7.1	This section should address the possibility that security vulnerabilities or usability or accessibility problems will be discovered, but that these problems do not constitute non-compliance with the applicable standards.
7.2	This section must clarify the extent of non-compliance with the VVSG that is required to decertify a voting system. Although the language of the second sentence is mandatory—"Systems *shall* be decertified . . ." (emphasis added)—the extent of violation is unclear because item (1) refers to applicable VVSG "standards" that are not met. How many applicable standards may a system fail to meet and still retain certification? Will the EAC view some kinds of non-compliance more harshly than others? Will the EAC weigh other circumstances (e.g., the proximity of an election) against a voting system's failure to meet applicable standards when deciding whether to decertify a voting system? These are questions that should be answered in this section, but are not. Clarifying the EAC's decertification policy in § 7.2 is also important because § 7.4.7.1 references this policy as the substantive standard for determining whether the EAC will move to decertify a system. Consistency across voting systems and EAC membership are important considerations here.
7.3.3.1	Clarify that the sources of information about possible non-compliance are not limited to the persons listed in this section. For example, computer security experts might help state or local elections officials test fielded voting systems. Reports from such experts might prove to be a valuable source of information about voting system non-compliance. In addition to requiring that information be relevant, this section should also require that it be judged reliable, rather than attributable, to serve as the basis for initiating and Informal Inquiry. This change would more clearly allow the EAC to act on information brought forward by internal whistleblowers that might wish to remain anonymous. Finally, this section should not provide for notification of the Manufacturer. Given the limited scope of an Informal Inquiry, notification at this stage is unnecessary and might impede the inquiry.

Section	Comments
7.3.4	The EAC should publish all Memoranda for the Record; or, at minimum, it should publish an annual report that states, separately for each registered Manufacturer, the reason for any Informal Inquiry into that Manufacturer's voting system, the disposition of each such Inquiry, and the reasons for that disposition.
7.4.4	Publish each notice of initiation of a Formal Investigation on the EAC Web site as soon as the notice is issued to the Manufacturer.
7.4.5.4	The last sentence of this section should be changed to read: "During the predecisional phase of an investigation, all investigative materials must be appropriately safeguarded."
7.4.5.5	Specify a sanction for refusals to cooperate with the investigation; such refusals should be grounds to initiate deregistration proceedings against a Manufacturer.
7.4.5.5	Add a section after 7.4.5.5.5 that reads: "Outside expert review. Investigators may consult individuals with expertise in a field relevant to some area of the investigation. These experts may be given access to any relevant investigative materials and may be asked to participate in the EAC's investigative activities."
7.4.7	This section should more clearly delineate the factual findings of an investigation from its interpretations of the Manual and other applicable regulations and laws.
7.4.7.1	Please see our comments to § 7.2.
7.4.8	This should state affirmatively that the report will be made public: "The report shall be made public when it is final."
7.6.2	The first sentence should read: "The Notice of Non-Compliance must also inform . . ."
7.6	The EAC must add a section to warn state and local elections officials who are contemplating the purchase of a voting system for which decertification is pending. The EAC could give this warning by maintaining a public list of each voting system that is under a Notice of Non-Compliance, or the EAC could send an announcement of each Notice to all state and local elections officials.
7.7.1	This section must include a provision for more thorough testing of proposed cures; otherwise, a cure could introduce modifications—even modifications that are unrelated to the defects found in testing—that do not receive the same level of scrutiny as the rest of the voting system. This section must fix a minimum number of days preceding a federal election before which any cure must be completed. If the cure is not completed by this deadline, the EAC must decertify the voting system in question. This section, in its current version, would maintain certification for a modified voting system, so long as all modifications are "in place before *any* individual jurisdiction

Section	Comments
	fielding the system holds a Federal election" (emphasis in original). This timetable would not necessarily allow a jurisdiction to test the modification, even if state law requires it to do so. In addition, unless this section creates a minimum time between completion of a cure and the next federal election, it is possible that the Manufacturer will not complete the cure, and that the voting system will be decertified, without leaving affected jurisdictions sufficient time to make alternative arrangements.
7.7.1.3	This section should require a VSTL to prepare a test plan and submit it directly to the EAC. This section also must require the Manufacturer to have the proposed cure tested by a VSTL; the current version of the Manual simply states that the Manufacturer must "provide for the testing of the system." Similarly, the Manual must require the VSTL to submit its test report directly to the Program Director.
7.7.1.6	This section should take into account the timing issues that we raise in our comments to § 7.7.1.
7.7.2.3	This section raises concerns similar to those that we discuss in our comment to § 6.9.3.3 and should be stricken.
7.7.1.6	The first sentence should read: "After receipt of the test report . . ."
7.8	This section should require the EAC to publish its Decision at the same time it sends the Decision to the Manufacturer.
7.9.1.1	This section should state that the EAC will publish each request for appeal of decertification upon receiving that request from the Manufacturer.
7.9.2.2	As we state in our comment to § 7.7.1.3, the record should not include the materials specified in that section.
7.9.3	A subsection should be added to require the EAC to publish each Decision on Appeal immediately after the Decision is made final.
7.10	Add to the effects of decertification: "The EAC will immediately add the voting system to a published list of decertified systems, which shall include the date of and reasons for decertification."
§ 8: QUALITY MONITORING PROGRAM	
8.6	The scope of review and testing in this section should be expanded. This could be done by replacing the third sentence with: "The EAC may elect to test a fielded system."
8.7.2	Allow any person who has direct experience with a voting system to report an anomaly in that system. Also, this section should provide for the confidentiality of reporters' identities. Elections officials, as well as the expanded range of reporters that we suggest, might provide lower quality information, or choose not to submit reports at all, if their names are publicly associated with a

Section	Comments
	specific report. The EAC would clear this obstacle to reporting by providing confidentiality for any reporter who chooses it.
8.7.3	First, expand the scope of reportable subject matter. The current language suggests a focus on reliability issues, but the EAC should accept reports about accuracy, security, accessibility, usability, and other problems. Second, clarify what constitutes a "disruption." It is unclear, for example, whether vote count disparities identified by manual audits, or votes recovered from redundant storage after failure of the primary storage system, result in "disruption" if they are resolved in manner that does not delay any part of the election process. Also, the line between "administrator error or procedural deficiencies" and voting system anomalies may be difficult to police. This section should provide additional guidance to better define "administrator error" and "procedural deficiencies."
8.7.4	Publish credible anomaly reports on the EAC Web site. This section already provides for wide distribution of these reports, leaving little risk to security or confidentiality in unlimited publication. Moreover, the EAC Web site could play a valuable role as a clearinghouse for anomaly reports.
§ 9: INTERPRETATION	
9.1	Expand the set of persons who are allowed to request an Interpretation. The touchstone of whether a request is appropriate should be whether the requester presents a clear factual situation relating to some provision of a voting system standard, rather than the identity of the requester.
9.3.1	This section incorrectly suggests that VSTLs may be agents of Manufacturers, a notion that is contrary to VSTLs' independence. This section should simply state that VSTLs may request Interpretations. In addition, this section should permit requests from any person who can satisfy the other requirements under § 9.3. For example, elections officials might serve as a rich source of factual situations to guide Interpretations.
9.3.4.2	Rejecting an Interpretation request because the issue in the request has "previously been clarified" could give an advantage to one Manufacturer over another. This situation could be improved by publishing all Interpretations. For information on this point, see our comments on § 9.7
9.5.1.2	The EAC should publish the request and the basis for its rejection.
9.7	This section should require the publication of all Interpretations.

Section	Comments
	Since § 9.3.4.2 states that the EAC will not issue an Interpretation for an issue that "have previously been clarified," it is essential to provide a public record of what those issues are and how they were clarified.
§ 10: TRADE SECRET, CONFIDENTIAL COMMERCIAL, AND PERSONAL INFORMATION	
10.2	FOIA is codified at 5 U.S.C. § 552, not 5 U.S.C. § 522.
10.3.1	This section should not declare entire categories of documents to be trade secrets. Although the examples given in §§ 10.3.1.1-4 may be trade secrets within the meaning of the relevant FOIA exemption (5 U.S.C. § 552(b)(4)), disclosures in other contexts or even the wishes of the submitter may destroy secrecy or confidentiality and require release of documents under FOIA.
10.3.1.3	If § 10.3.1 is retained, replace this section with "Voting system source code."
10.6.2.2	The Manual must provide information requesters an opportunity to respond to additional information provided by a Manufacturer. In addition, the Manual must provide clear guidance about the EAC's procedures for determining whether information is exempt from disclosure and establishing a record for these decisions.
10.7	This section should specifically state that the EAC will redact information that it determines to be trade secrets or confidential commercial information and release redacted versions of documents that contain such information.