ACCURATE

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

Public Comment on the Uniformed and Overseas Citizens Absentee Voting Act Pilot Program Testing Requirements[*]

Submitted to
The United States Election Assistance Commission

April 30, 2010

[*] This material is based upon work supported by the National Science Foundation under A Center for Correct, Usable, Reliable, Auditable and Transparent Elections (ACCURATE), Grant Number CNS-0524745. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation. This public comment narrative was prepared by Aaron Burstein and Joseph Lorenzo Hall in consultation with the ACCURATE Principal Investigators and Advisory Board members Whitney Quesenbery, Ron Rivest and Noel Runyan.

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://chil.rice.edu/byrne/

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

Jeremy Epstein
Computer Science Laboratory
SRI International
jepstein@csl.sri.com
http://www.csl.sri.com/people/epstein/

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

Deirdre K. Mulligan
School of Information
University of California, Berkeley
dkm@ischool.berkeley.edu
http://www.ischool.berkeley.edu/
people/faculty/deirdremulligan

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

Natarajan Shankar
Computer Science Laboratory
SRI International
shankar@csl.sri.com
http://www.csl.sri.com/people/shankar/

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

1 Introduction

1.1 ACCURATE Background

A Center for Correct, Usable, Reliable, Auditable and Transparent Elections (ACCURATE),[1] a multi-institution, interdisciplinary, academic research center funded by the National Science Foundation's (NSF) "CyberTrust Program,"[2] appreciates the opportunity to provide these comments on the draft Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements[3] to the Election Assistance Commission (EAC).

ACCURATE was established in 2005 to conduct fundamental research into methods for improving voting technology. ACCURATE's Principal Investigators direct research investigating software architecture, tamper-resistant hardware, cryptographic protocols and verification systems as applied to electronic voting systems. Additionally, ACCURATE evaluates voting system usability and how public policy, in combination with technology, can better support elections.

Since receiving NSF funding in 2005, ACCURATE has made many important contributions to the science and policy of electronic voting.[4] With experts in computer science, systems, 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 strengthen the specifications and requirements that ensure the functionality, accessibility, security, privacy and trustworthiness of our voting technology.

1.2 UOCAVA Pilot Program Requirements

The EAC's first effort to set requirements for voting systems that will serve overseas voters—including military service members and their families—marks an important milestone in the development of voting system technical requirements. Voting systems that help overseas voters cast timely ballots in a manner that is secure, accessible, auditable, and secret would constitute a major improvement over the situation in which too many of these voters find themselves now: effectively disenfranchised because of their location.[5]

Additionally, the EAC's draft UOCAVA Pilot Program Testing Requirements ("the UOCAVA Draft" or "the Draft") follows the lead of the draft for the "next generation" Voluntary Voting System Guidelines ("VVSG II") on several critically important technical issues.[6] Overseas voting amplifies many of

[1] *See:* `http://www.accurate-voting.org/`.

[2] National Science Foundation Directorate for Computer & Information Science & Engineering, CyberTrust, *see:* `http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=13451&org=CISE`.

[3] U.S. Election Assistance Commission. *Uniformed And Overseas Citizens Absentee Voting Act (UOCAVA) Pilot Program Testing Requirements*. Mar. 2010. URL: `http://www.eac.gov/program-areas/voting-systems/docs/requirements-03-24-10-uocava-pilot-program/attachment_download/file`.

[4] See ACCURATE's annual reports: A Center for Correct, Usable, Reliable, Auditable and Transparent Elections. *2006 Annual Report*. Jan. 2007. URL: `http://accurate-voting.org/wp-content/uploads/2007/02/AR.2007.pdf`; A Center for Correct, Usable, Reliable, Auditable and Transparent Elections. *2007 Annual Report*. Jan. 2008. URL: `http://accurate-voting.org/wp-content/uploads/2008/01/2007.annual.report.pdf`; A Center for Correct, Usable, Reliable, Auditable and Transparent Elections. *2008 Annual Report*. Jan. 2009. URL: `http://accurate-voting.org/wp-content/uploads/2008/12/2008annualreport.pdf`

[5] Kevin J. Coleman. *The Uniformed and Overseas Citizens Absentee Voting Act: Overview and Issues*. Congressional Research Service. Nov. 2009. URL: `http://assets.opencrs.com/rpts/RS20764_20091104.pdf`, at 6.

[6] ACCURATE is strongly supportive of the draft VVSG II (released in August 2007), particularly the essential requirements of software independence, adversarial vulnerability testing (a/k/a "OEVT testing"), usability benchmark testing and volume testing. *See:* A Center for Correct, Usable, Reliable, Auditable and Transparent Elections. *Public Comment on the Voluntary Voting System Guidelines, Version II (First Round)*. May 2008. URL: `http://accurate-voting.org/wp-content/uploads/2008/05/accurate_vvsg2_comment_final.pdf`

the security, reliability, usability, and accessibility challenges that confront U.S. elections. We believe that the technical foundations of the VVSG II that have been incorporated into the Draft will considerably benefit overseas voters and the U.S. election system. Specifically, the Draft would require:

1. that systems operate in a controlled, supervised environment (see § 2 below);
2. auditability through a voter-verified paper record requirement (see § 3 below);
3. basic usability testing, though we recommend expanded usability and accessibility requirements (see § 4 below); and,
4. penetration testing and threat modeling (see § 5 below).

There are, however, a number of issues in the Draft that the EAC should address. We highlight two of them here. First, though we recognize the need to create a pilot system certification process that is "quicker and less expensive than the regular process currently used for conventional systems with an expected life of more than 10 years,"[7] the EAC should also recognize that pilot systems have the potential to find wider application.[8] Thus, maintaining the rigor of testing that the Draft prescribes is critical. In addition, publishing as much data as possible from pilot system certification testing and actual pilot system deployments will facilitate independent review and analysis. The history of electronic voting systems in the past decade has shown that continuing public review is essential for oversight and the improvement of voting systems.[9] Second, the Draft needs to close the loop between voter-verified paper records and post-election audits. As we discuss further in Section 3, ballots cast through a remote electronic voting system should be as auditable as votes cast through more conventional means. This is important to protect the integrity of remotely cast ballots, as well as any election in which they are cast.

1.3 A Note About Process

The process for commenting on the UOCAVA Draft was an unfortunate departure from the EAC's past processes for commenting on voting system guidelines. The EAC released the Draft on or around March 26, 2010, and initially set a comment deadline of April 9, 2010. However, the Draft was not noticed in the Federal Register until March 31, 2010,[10] effectively extending the deadline to April 15, 2010. Finally, at the moment of the deadline on April 15, the EAC notified submitters that there had been an error and that the comment period was to be a 30-day comment period, ending on April 30.[11]

[7] U.S. Election Assistance Commission, *EAC UOCAVA Pilot Program Requirements*, see n. 3, § 1.1.3.

[8] We address procedural issues in: A Center for Correct, Usable, Reliable, Auditable and Transparent Elections. *Public Comment on the Voting System Pilot Program Testing & Certification Manual*. Apr. 2010. URL: `http://accurate-voting.org/docs/comments/accurate_vspptcm_comments.pdf`

[9] *See, e.g.*, California Secretary of State. *Top-To-Bottom Review of California's Voting Systems*. Mar. 2007. URL: `http://www.sos.ca.gov/elections/elections_vsr.htm`; Patrick McDaniel, Matt Blaze, Giovanni Vigna, et al. *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing (Academic Final Report)*. Ohio Secretary of State. Dec. 2007. URL: `http://www.sos.state.oh.us/sos/info/EVEREST/14-AcademicFinalEVERESTReport.pdf`; Ryan Gardner, Alec Yasinsac, Matt Bishop, Tadayoshi Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke. *Software Review and Security Analysis of the Diebold Voting Machine Software*. July 2007. URL: `http://election.dos.state.fl.us/pdf/SAITreport.pdf`

[10] Notice: Request for Substantive Comments on the EAC's Proposed Requirements for the Testing of Pilot Voting Systems To Serve UOCAVA Voters, 75 Fed. Reg. 16088, 16090 (Mar. 31, 2009), see: `http://www.gpo.gov/fdsys/pkg/FR-2010-03-31/pdf/2010-7199.pdf`.

[11] This last-minute extension was frustrating. Commentors that could have planned to use a 30-day comment period were instead forced to rush comments under the exceptional 15-day period. Some who did manage to submit comments by the April 15 deadline felt that their submissions were substandard and would not have submitted subpar public commentary if the EAC had caught this error earlier.

Even this 30-day comment period was too short for a document of the UOCAVA Draft's complexity and importance. By way of comparison, the EAC allowed 180 days for comments on VVSG II and 120 days for VVSG 1.1. Though a 30-day comment period[12] is better than 15, it still provides insufficient time to analyze a standard that involves the relatively unexplored territory of transmitting ballots over the Internet.

It is our hope that the Draft is just a beginning, and that the results of any pilots conducted under the adopted UOCAVA requirements will initiate a more extensive process of refinement, public analysis, and public participation.

2 The Focus on Controlled, Supervised Voting Systems Is Appropriate

We are encouraged to see that the scope of UOCAVA pilot project activities will be limited to a subset of possible remote voting architectures. Specifically, § 1.1.3 states that the scope of these requirements are confined to **supervised** polling place environments on **controlled** voting system platforms.

Supervised polling place environments employ a team of dedicated pollworkers or election staffers that work to monitor and enforce procedures. For example, well-trained staff can help to minimize the opportunity for vote-buying and coercion by making sure that only one person is in a voting both at a time and that voters do not leave the premises with unvoted ballots or election media. In addition, monitored polling places will pose a greater challenge to individuals who might exploit physical access to election equipment in order to mount attacks such as corrupting vote tallies or rendering a voting system inoperable (i.e., causing a denial of service).

A controlled voting system platform is one where an election authority controls the configuration, maintenance and operation of the voting system. If voting were to be conducted on an uncontrolled platform, such as on voters' personal computers or computers at commercial establishments such as Internet cafes, the voting system would have to be designed to mitigate the large variety of fundamental security problems associated with consumer computer usage, such as unpatched operating systems, viruses, eavesdropping software and insecure local networks. As ACCURATE PIs Rubin and Wagner and Advisory Board members Jefferson and Simons pointed out in the 2004 SERVE Security Report, the general problem of securing computing services on arbitrary personal computers over public networks is very difficult.[13]

Limiting the scope of this requirements to controlled, supervised architectures is prudent; it is best to begin pilot projects such as these in more secure, limited configurations before attempting configurations that pose fundamental limits to the integrity of elections. The Draft, however, should state explicitly that no other type of voting system can be tested and certified to these requirements. An explicit statement to this effect in § 1.1.3 would suffice.

3 The Voter-Verified Paper Record Requirement Is Strongly Warranted

The UOCAVA Draft follows the vast majority of states in requiring voting systems that record votes through an electronic interface to generate a separate, voter-verifiable paper record (VVPR) of each

[12] 30 days for notice and public comment is the minimum allowed by the EAC's Notice and Comment Policy without a waiver. *See:* U.S. Election Assistance Commission. *Notice and Comment Policy (as adopted)*. Sept. 2008. URL: `http://www.eac.gov/about/docs/proposed-notice-and-public-comment-policy-finalchanges-published.pdf/attachment_download/file`, at 3–4, § V.A.

[13] David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner. *A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)*. 2004. URL: `http://www.servesecurityreport.org/paper.pdf`.

ballot.[14] It is difficult to overstate the importance of this requirement: the history of paperless DREs' unreliability, the inconclusiveness of post-election examinations of purely electronic systems, and the demonstrated potential for attacks on software and hardware that are undetectable without audits all counsel strongly in favor of this requirement.[15]

The Link Between Paper Records and Auditing. As ACCURATE has stated in previous comments to the EAC, a principal purpose of an independent, voter-verified record—such as a VVPR—is to facilitate post-election audits that are capable of detecting errors or faults in voting system software.[16] Put simply, a VVPR system is not secure without audits. This is true irrespective of whether the system is designed to cast ballots electronically from overseas or in a traditional voting precinct.

Subject to the recommendations we make below, we believe the UOCAVA Draft's technical requirements for VVPRs are adequate. We also support the requirement that paper records "be retained for later auditing or recounts, as specified by state law."[17] In addition, we recognize that the Draft deals with technical requirements, not election administration procedures, whether they involve officials from the Federal Voting Assistance Program (FVAP) or from the states.[18]

Nonetheless, given that post-election audits are central to the security of any VVPR-based system, we point out that there are significant gaps between the Draft and a program for effectively incorporating ballots cast on the voting systems envisioned by the Draft into post-election audits. To be used in a post-election audit, these records must reach election jurisdictions during the canvass period, which may be as short as ten days (e.g., Florida) or as long as 28 days (e.g., California). The Draft understandably does not provide a mechanism for returning VVPRs to voters' home jurisdictions. The Draft, however, could facilitate this process by requiring manufacturers to document how their system supports auditing processes, for example, quick and accurate sorting of VVPRs.

We also suggest that Draft § 2.6 advise that pilot projects develop a protocol for returning paper records to voters' home jurisdictions.[19]

Manufacturers should be required to provide the EAC, VSTLs, and state election officials with suggested chain-of-custody procedures for the paper records and paper record canisters. Chain-of-custody is an important aspect of maintaining the integrity of ballot materials in existing elections It is even more critical for remote voting, which will involve much larger distances and, at some point, dividing up the paper records from each voting system so that they can be delivered to individual election jurisdictions.

Requiring these descriptions as part of the Technical Data Package—perhaps in the System Security Specifications (§ 8.3.3)—and making them part of the conformity assessment would advance pilot systems' support for post-election auditing.

Finally, we note that post-election auditing has only been performed once with the type of remote

[14] According to VerifiedVoting.org, only 12 states lack a uniform state requirement for VVPRs. *See* `http://www.verifiedvoting.org`.

[15] For a review of the security and reliability deficiencies of purely electronic systems, see: A Center for Correct, Usable, Reliable, Auditable and Transparent Elections, *Public Comment on VVSG II*, see n. 6, 3-4.

[16] *See* ibid., 2-8. As we explained in that document, the term "post-election audit" encompasses more than checking for consistency between an electronic vote count and a tally of paper records. For example, such audits might include examining audit logs to detect anomalous events. For further comments about the UOCAVA Draft's treatment of audit logs, see Section 6, below.

[17] U.S. Election Assistance Commission, *EAC UOCAVA Pilot Program Requirements*, see n. 3, § 2.6.3.

[18] State audit requirements are highly variable, ranging from mandatory post-election audits with provisions to escalate their scope under certain conditions, to more-or-less outright bans on post-election audits.

[19] The *Voting System Pilot Program Testing & Certification Manual* should make the review of this protocol part of the testing and certification process.

voting system envisioned in the Draft.[20] That system was designed for limited use—restricted to one federal election for a single jurisdiction—and no post-election report was publicly released. Pilot programs such as this UOCAVA Pilot Program present valuable opportunities to learn about logistical considerations of auditing remote voting systems, as well as standard audit-related information related to system accuracy and reliability. While we do not have specific technical requirements to recommend, we urge the EAC—and its partners in the UOCAVA Pilot Program, FVAP and NIST—to study these aspects of securing remote voting systems, should a UOCAVA pilot proceed. We also urge the EAC to work with these partners to issue a timely and public post-election report, including an analysis of any audits conducted and any post-election assessment activity.

The Need for Physically Robust Paper Records. Additionally, the Draft should go further to require paper records that are themselves robust and support other needs of the election system, such as recounts and post-election audits. The Draft does not prescribe a VVPR design,[21] but currently the main options are cut-sheet and paper-roll systems.[22] Cut-sheet paper records would have significant advantages over paper-roll records for recounts and post-election auditing.[23] Specifically, they are easier to separate according to voters' home election jurisdictions, and easier to use in hand audits. This is an important consideration, given that the same vote capture device might serve voters who are registered in many different jurisdictions.

Irrespective of the printing technology that a vote capture device uses, the final requirements should include standards for paper record durability. The draft VVSG II provides a requirement that we suggest adopting for UOCAVA pilot systems: paper records must "remain unchanged for minimally 22 months unaffected by power failure, software failure, or other technology failure."[24] The Draft should further emphasize that this standard applies to the human- and machine-readable portions of the VVPR. During testing and certification, the EAC should also take into account the likelihood of prolonged exposure to the environmental extremes (heat, humidity, etc.) that these devices and paper records are likely to encounter.

Supporting Paper Records and Audits with Electronic Data. The Draft generally contains sound requirements for generating electronic data to support auditing. However, below we suggest several ways that the Draft could be improved in this area.

- Scope (§ 2.6.1): The distinction between a manual tally audit and a ballot image audit needs to be clarified. We suggest changing subsections (a) and (b) to read:

  > (a) Hand audit – Validate electronic tabulation results via comparison with results of a hand tally of randomly-selected paper records; and
  >
  > (b) Ballot image audit – Random sampling comparison of the contents of ballot images and the corresponding paper records.

[20] *Procedures and System Description for Secure Remote Electronic Transmission of Ballots for Overseas Civilian and Military Voters*. Operation BRAVO Foundation. June 2008. URL: http://election.dos.state.fl.us/voting-systems/pdf/ODBPplanJune_19.pdf.

[21] U.S. Election Assistance Commission, *EAC UOCAVA Pilot Program Requirements*, see n. 3, § 2.6.3.

[22] Technical Guidelines Development Committee. *Voluntary Voting System Guidelines Recommendations to the Election Assistance Commission*. Aug. 2007. URL: http://www.eac.gov/files/vvsg/Final-TGDC-VVSG-08312007.pdf, § 1-4.4.2.4.

[23] The Draft anticipates such records. For example, § 2.6.3.4 sets requirements for labeling ballot records that span multiple sheets of paper. However, none of the language in the Draft suggests that such records are mandatory.

[24] Technical Guidelines Development Committee, see n. 22, § 1-4.4.1-A.5.

- Electronic records (§ 2.6.2): The EAC should require electronic records (§ 2.6.2.1) to be exported in a structured, open format. The Draft sets such a requirement for audit logs (see § 5.6),[25] and this section should parallel those requirements.[26] In addition, § 2.6.2 should explicitly state that cast vote records (CVRs) are among the records that must be exportable in a structured, open format.

- The intended purpose and meaning of the last paragraph of § 2.6.2 (beginning with "The following requirements. . . ") are unclear. This appears to be a drafting problem.

- Linking the electronic CVR to the paper record (Section 2.6.3.7(b)) requires the paper record to "[i]dentify whether the paper record represents the ballot that was cast." We recommend adding a suggestion to comply with the requirement, such as: "For example, the voting system could print 'VOID' across any spoiled paper record." The absence of this mark would then indicate that the corresponding electronic record was cast. Our suggested wording leaves open the possibility of other methods of identifying paper records to electronic CVRs.

4 Usability and Accessibility Requirements Need Improvement

It is laudable that the UOCAVA Draft includes some basic usability testing requirements in § 3. However, it pays scant attention to usability requirements and entirely omits accessibility testing and requirements.

The omission of accessibility is a significant deficiency. The population of uniformed overseas voters, as current soldiers or former soldiers, presumably have a significant rate of disability. We were unable to find any useful statistics or research concerning disability rates of overseas military personnel. Unless there is evidence to the contrary, the requirements should be based on the assumption that UOCAVA voters are at least as likely as domestic voters to require accessibility support. Indeed, given the large fraction of UOCAVA voters who are in the military or who are engaged in dangerous work, it would be prudent to assume (in the absence of contrary data) that UOCAVA voters are *more* likely than domestic voters to need such support. Certainly, wounded soldiers can spend significant amounts of time at medical facilities close to the theater of their deployment. Soldiers with severe wounds are often relocated to U.S. medical facilities outside of their home jurisdictions. It can also be difficult to use a touch screen when in an arm sling, or at standing height when in a wheelchair. Accessibility requirements and evaluation of those requirements are crucial in this respect. (There may also be legal implications of the standard not addressing accessibility due to requirements of the Help America Vote Act and the Rehabilitation Act.[27])

We are also disappointed that the usability requirements in the Draft seem to be chosen selectively from the VVSG II usability section. It is not clear why this subset of requirements from the VVSG II's comprehensive usability framework was selected. The Draft's requirements are a good start, but many known usability issues, which would be covered under the VVSG II, remain unaddressed in the UOCAVA Draft. We suggest revisiting these requirements.

[25] See, in particular, § 5.6.1.5: "The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format."

[26] For more detailed suggestions about how to specify these requirements, A Center for Correct, Usable, Reliable, Auditable and Transparent Elections. *Public Comment on the Voluntary Voting System Guidelines, Version 1.1*. Sept. 2009. URL: `http://accurate-voting.org/wp-content/uploads/2009/09/ACCURATE-vvsgv11-final.pdf`, at 4-7.

[27] HAVA's § 301 requirements (42 U.S.C. § 15481(a)) require accessible voting be provided in federal elections and the § 508 requirements of the Rehabilitation Act (29 U.S.C. § 794(d)) require that any federal information and communications technologies must be accessible.

The lack of usability benchmarks and benchmark testing, championed in the VVSG II, is a source of concern. From a usability standpoint, the usability benchmarks and testing mechanisms are probably the single most valuable piece of the VVSG II (outside of the enhanced accessibility requirements) in terms of broadening enfranchisement and reducing the number of lost votes. Providing requirements and testing for holding voting equipment to objective usability testing standards is critically important to ensuring usable systems.

Finally, the requirements as written might simply not be met. Most of the requirements are listed as "functional," and from years of both research and practice in usability, we know that "functionality" does not equal "usability." More troublesome is that the manufacturer is the test entity for all of these requirements. Particularly given the vagueness with which many of these requirements are written, history indicates that such requirements are unlikely to be met without some kind of external review. Even if the Draft does not incorporate explicit benchmarks, it should provide some kind of explicit external oversight to ensure that manufacturers take these requirements seriously.

We include additional commentary on specific sections with the usability requirements below in the Appendix.

5 Improvements in Security Specification and Testing

ACCURATE has in past comments highlighted a number of enhancements needed in the EAC testing and certification process with respect to security.[28] Two elements of our past comments are included in the UOCAVA Draft: threat modeling documentation and adversarial vulnerability testing.

ACCURATE has long called for requiring voting system manufacturers to articulate the threats their voting systems are designed to protect against. In computer security, this process is called threat modeling. It involves thinking as a possible attacker would think in order to identify how an attacker's goals (subversion, denial of service, etc.) might be accomplished. Section 8.5.1.2 of the UOCAVA Draft requires manufacturers to include a "Security Threats Controls" document as part of the Technical Data Package that "identifies the threats the system protects against and the implemented security controls on system and system components." While short on details, this is a requirement for manufacturers to both provide their threat models for these systems and describe the controls that mitigate or minimize these threats.

The EAC could make this requirement more effective with a few modest changes. First, the description of this threat modeling document is potentially under-inclusive, since there could be plausible threats that the system does *not* protect against. The document should clearly identify threats the system's engineers and designers considered out of scope for their security architecture. Second, since the threats to Internet voting systems are radically different from those to a traditional precinct-based (or vote-by-mail) voting system, threat models need to be very explicit about possible threats> The threat model should be required specifically to cover and identify insider and outsider threats and to provide a qualitative description of the skill and motivation of anticipated attackers. These changes would dramatically improve the utility of this document to testing laboratories, EAC technical evaluators and state-level voting system examiners.

The UOCAVA Draft includes strong requirements for penetration resistance (§ 5.9.1) as well as *testing* resistance to penetration (§ 5.9.2). (The UOCAVA Draft refers simply to "penetration resistance" and testing. The draft VVSG II calls a similar set of requirements "Open-Ended Vulnerability Testing." We prefer the more precise term, "adversarial vulnerability testing.") The Draft's requirements recog-

[28] A Center for Correct, Usable, Reliable, Auditable and Transparent Elections. *Public Comment on the 2005 Voluntary Voting System Guidelines*. Sept. 2005. URL: `http://accurate-voting.org/accurate/docs/2005_vvsg_comment.pdf`, § IV; Technical Guidelines Development Committee, see n. 22, § 3.

nize that "white box" penetration testing, in which the penetration team is allowed access to knowledge that insiders would have, is a highly effective way to find vulnerabilities that might not have been obvious or practical for attackers with outsider (or "black box") knowledge.[29] It is also best practice to allow, as the UOCAVA Draft does in § 1.3.6.2, forms of testing with broad scope, like penetration testing, to call into question conformance of higher-level requirements: "However, if non-conformance with a higher-level requirement is determined through any other means (e.g., OEVT testing, inspection, etc.) then the voting system is deemed not to conform to that higher-level requirement."[30]

The EAC should also require manufacturers to keep track of these vulnerabilities (and their resolution) through an incident handling mechanism. This mechanism would record information describing the vulnerability in terms of voting system software, hardware, or COTS components; how the manufacturer has resolved or will resolve the problem; and how it will get information and fixes to their customers. Moreover, incident tracking should be a requirement for *all* vulnerabilities, not just those discovered during testing. One way to formulate this requirement is to require manufacturers to submit documentation of an incident handling mechanism part of the § 8's TDP requirements.

Both penetration testing and threat modeling documentation are welcome features in both the requirements for these systems and for the evaluation of these systems' vulnerabilities. They reflect expert opinion that security standards such as those in the UOCAVA Draft—as well as other system security standards such as the Common Criteria and the TCSEC Rainbow Series[31]—can still fail to eliminate critical vulnerabilities that a computer security expert may be able to imagine during a threat-aware "white box" system security review. Ultimately, in order to effectively expedite testing and certification, it will be necessary to move to "goal-based" or "case-based" certification,[32] where vendors are required to submit affirmative argumentation that provides direct evidence that the system fulfills a set of *claims* about *properties* their system honors. The Pilot Program certification regime would be an appropriate place to test such new paradigms before adapting them for the larger EAC testing and certification process.

6 Conclusion

We welcome these draft standards, and overall we find many elements of the draft very positive. ACCURATE appreciates the opportunity to comment on the UOCAVA Draft. We would be happy to answer any questions the EAC has about our comments. We also look forward to analyzing the outcome of any pilot conducted according to the final requirements, as well as any future revisions to the requirements themselves.

[29] The California Top-To-Bottom Review of voting systems, the Ohio EVEREST Review of voting systems and the various voting system reviews conducted by the Florida Department of State all operated under a "white box" review model and substantially increased the knowledge about the level of vulnerability in these systems over what we would expect if these reviews operated under a "black box" model. *See, e.g.*, California Secretary of State, see n. 9; McDaniel, Blaze, Vigna, et al., see n. 9; Gardner, Yasinsac, Bishop, Kohno, Hartley, Kerski, Gainey, Walega, Hollander, and Gerke, see n. 9

[30] This is the one place in the document where the phrase "OEVT testing" is used instead of "penetration testing". Given that the rest of the document is standardized on using "penetration testing" we suggest this be changed.

[31] International Standards Organization. *The Common Criteria for Information Technology Security Evaluation, Version 2.1, ISO 15408*. ISO/NIST/CCIB. 2000; National Computer Security Center. *Department of Defense Trusted Computer System Evaluation Criteria*. National Computer Security Center, 1985.

[32] Daniel Jackson. "A direct path to dependable software". *Commun. ACM* 52:4, 78–88 (2009). URL: http://doi.acm.org/10.1145/1498765.1498787.

Appendix: Section-Specific Comments

This section provides on comments on more specific issues in the UOCAVA Draft.

- **Interaction with Ballot Definition Sources:** Voters who use remote electronic voting systems will need to be connected to the appropriate ballot definition/ballot style for their locality. That is, the voting system will need to "know" the appropriate ballot style to serve to the voter. The proper place to set these requirements is in this document, but we find the Draft short on details. More specifically, the Draft does not specify how remote electronic voting systems will interface with "stores" of ballot definitions either held by FVAP or states (or localities). It is also unclear *when* in the voting process such interactions will take place. The Draft should also clarify whether the voting system can provide its own infrastructure for caching ballot definitions to provide a buffer against unavailability of the ballot definition store.

- **Voting System Operating Capacities (§ 2.2):** This section should be more specific about how to measure the voting system's capacity, e.g., by requiring a manufacturer to specify the number of ballots it can handle (§ 2.2.1).

  Also, the requirement to "provide notice" (§ 2.2.2) when the system is approaching capacity is inadequate. In at least one instance of early voting, the number of ballots cast exceeded the capacity of the voting system, resulting in lost votes.[33] It is unclear whether a warning would have avoided this problem. Instead, the voting system should be required not to present ballots to voters when it does not have the capacity to store additional votes.

- § 2.5.1.5.2: The language here mentions a "digital envelope," but the meaning of this term is unclear. We suspect it is some form of signed and encrypted ballot that also includes voter identification information in some form in an unencrypted (and separable) manner. The Glossary should provide a definition.

- § 3.3: "Clarity" is not operationally defined. At minimum, this section should specify that the requirement for clarity applies to all voters who use the system,[34] irrespective of their language or mode of interaction with the voting system. Clarity of poll worker instructions is another critical consideration.[35]

- § 3.4.1.1:

  - (a) Providing a "consistent relationship between the names of the candidates and where to cast a vote" does not provide a strong enough usability requirement. This relationship might be consistently confusing, for example.

[33] *More than 4,500 North Carolina Votes Lost Because of Mistake in Voting Machine Capacity*. USA Today (Associated Press). Nov. 2004. URL: `http://www.usatoday.com/news/politicselections/vote2004/2004-11-04-votes-lost_x.htm`.

[34] Janice Redish, Dana Chisnell, Ethan Newby, Sharon Laskowski, and Svetlana Lowry. *Report of Findings: Use of Language in Ballot Instructions*. NISTIR 7556. National Institute of Standards and Technology, 2009. URL: `http://vote.nist.gov/NISTIR-7556.pdf`; Janice Redish and Sharon Laskowski. *Guidelines for Writing Clear Instructions and Messages for Voters and Poll Workers*. NISTIR 7596. National Institute of Standards and Technology, 2009. URL: `http://vote.nist.gov/032906PlainLanguageRpt.pdf`.

[35] Dana Chisnell, Susan Becker, Sharon Laskowski, and Svetlana Lowry. "Style Guide for Voting System Documentation: Why User-Centered Documentation Matters to Voting Security". *USENIX/ACCURATE/IAVoSS Electronic Voting Technology Workshop/Workshop on Trustworthy Elections 2009 (EVT/WOTE' 09)* (Aug. 2009). URL: `http://www.usenix.org/events/evtwote09/tech/full_papers/chisnell.pdf`.

  - (c) Three seconds is not fast enough for system response time. People perceive meaningful delays such that they are likely to re-enter inputs and, in general, make mistakes at lags considerably shorter than this. The maximum lag for touchscreen interfaces should probably be no longer than 250 ms. For audio interfaces, the maximum tolerable response time is much shorter, approximately 100 ms. This section of the requirements should recognize that different modes of interaction require different maximum lag values and it should list maximum lag values for known modes of interaction.[36]

- § 3.4.1.2(a) should specify not only minimum distances between button centers, but also minimum distances between button edges. 0.3 inches is a suitable minimum for distances between button edges.

- § 3.5: While there is a requirement that no race be split across screens, the Draft lacks a requirement for a consistent number of races race per screen. This should be specified; one race per screen is probably best unless the screens are very large.

- 3.5.1.1: "Scrolling" is not operationally defined. One could argue that "next"/"previous" buttons is a form of discrete scrolling. Unless the intent is to require a full-face ballot, this requirement needs to be clarified.

- 3.5.1.2: In principle this is a good requirement, but it will be at odds with some local election laws that specify an extremely large number of candidates (e.g., the California gubernatorial recall election). It appears impossible to meet this requirement in all cases; there should probably be exception language for certain conditions.

- § 3.6 provides some basic ballot legibility requirements but is too vague in many places. For example, what are the operational definitions of "clearly legible" and "possible to clearly distinguish"?

  Setting a minimum text size without setting a minimum contrast ratio (at least 3:1) will not guarantee readable text. Note that this is an example of using only a subset of the draft VVSG II, which does specify a minimum contrast ratio but also specifies that voters must have the ability to select a larger font.

- The requirements in §§ 4.6.2-.3 and §§ 4.7.2.7-.8 are assigned to the VSTL for testing, while the surrounding requirements are assigned to the manufacturer. It would be helpful if the requirements document stated a rationale for this assignment.

- § 5.1.2.9: The intended meaning of this requirement ("The voting system SHALL log a notification when any account identification is locked.") is unclear. Perhaps the intent is to say that "the voting system shall log a notification when any account has been locked out due to events specified in § 5.1.2.8."

- § 5.2.1.1: This section should explain what an "authentication strength of 1/1,000,000" means by defining the term, pointing to the Glossary where the term is defined, or citing a standard or document that explains authentication strength.

[36] Vendors and VSTLs can use the EAC's Request for Interpretation process if they use a mode of interaction that is not listed in the standard. U.S. Election Assistance Commission. *Voting System Pilot Program Testing & Certification Manual*. Apr. 2010. URL: `http://www.eac.gov/News/docs/voting_system_draft_pilot_program_testing_and_certification_manual-03-31-10-final-public-comment.pdf/attachment_download/file`, at § 7 ("Requests for Interpretation")

- § 5.5.1.2: We recommend changing this language to read: "[. . .] shall use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, *including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0)*" (added text emphasized).

  The issue here is that a significant flaw in the basic TLS *protocol* was recently found that is only mitigated by a "Renegotiation Info" extension to the protocol, as outlined in RFC 5746.[37] However, there is a more general problem that our proposed wording seeks to cure: problems with cryptographic protocols can arise from both *protocols* and *implementations*. This requirement should be written so that the versions of specific protocols *and* implementations are current as of the date of submission.

- § 6: This section should include an introduction to explain that these requirements apply to *vendor-internal* QA processes.

- § 9.4.5.2: This requirement to document the procedure for scanning and performing optical character recognition lacks an underlying technical requirement. The most obvious place for such a requirement would be § 2.6.3, which sets forth requirements for paper record contents and format. However, § 2.6.3 divides information into "human-readable" and "non-human-readable" or (its apparent equivalent) "machine-readable" categories. The EAC should add a requirement stating that the human-readable part of the ballot be suitable for scanning and optical character recognition.

[37] Eric Rescorla, Steve Dispensa, Marsh Ray, and Nasko Oskov. *RFC 5746: Transport Layer Security (TLS) Renegotiation Indication Extension*. Feb. 2010. URL: `http://tools.ietf.org/html/rfc5746`.