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

PUBLIC COMMENT ON REQUEST FOR INFORMATION: GUIDELINES FOR THE USE OF ELECTRONIC VOTING SYSTEMS IN UNION OFFICER ELECTIONS*

Submitted to
U.S. Department Of Labor,
Office of Labor-Management Standards

March 14, 2011

*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 was prepared by Joseph Lorenzo Hall in consultation with the ACCURATE Principal Investigators and ACCURATE Advisory Board Member David Jefferson.

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, appreciates the opportunity to provide public comment to the Department of Labor, Office of Labor-Management Standards (OLMS) in its Request for Information (RFI) on Guidelines for the Use of Electronic Voting Systems in Union Officer Elections.[2]

ACCURATE was established in 2005 to research methods for improving voting technology in government elections. ACCURATE's Principal Investigators direct research into 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 2005, ACCURATE has made many important contributions to the science and policy of electronic voting.[3] 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 OLMS as it seeks to improve the administration of union officer elections.

1.2 Overview

ACCURATE's expertise is in voting technology, policy and usability as applied to government elections. We are not generally familiar with union elections; however, from the RFI narrative, it appears that the controlling law and regulations are similar in effect to the requirements for civic elections, if not substantially more uniform given the federal scope of OLMS compared with the local and state variation of government election administration.

In summary, electronic voting is an extremely difficult computer-facilitated activity to assure with confidence. ACCURATE recommends that voter-verified paper records (VVPRs) be required for voting systems involved with critical elections. Further, VVPRs are not meaningful themselves without robust audit processes that serve as a check on the voting system, ensuring that the reported election outcome is correct. We strongly urge the Department of Labor to refrain from issuing guidelines that permit internet voting, as in many respects there are no effective methods for ensuring security, integrity and reliability of such systems.

In the following comments, we will attempt to apply our expertise and experience to the 24 questions listed in the RFI. As best as possible, we will attempt to note where differences between labor and governmental elections might be relevant from a technical or policy perspective.

2 OLMS' RFI Questions

In the following enumerated sections, we will attempt to answer each of the 24 RFI questions, briefly, while pointing to further work in areas that might be helpful for OLMS to review. Some of the subject matter in subsequent questions will overlap with that from previous questions; in those cases we will reference the previous question.

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

[2] Guidelines for the Use of Electronic Voting Systems in Union Officer Elections, 76 Fed. Reg. 1559–1564 (Jan. 11, 2011) (amending 29 CFR pt. 452), *See:* `http://edocket.access.gpo.gov/2011/pdf/2011-311.pdf`.

[3] See ACCURATE's list of publications (`http://accurate-voting.org/pubs/`), reports & commentary (`http://accurate-voting.org/pubs/reports/`) and testimony (`http://accurate-voting.org/pubs/testimony/`).

1. *Should the Department issue guidelines concerning the use of electronic voting systems in union officer elections? What specific issues concerning electronic voting systems should be addressed? What specific standards should be included in the guidelines?*

Yes, OLMS should issue guidelines on the use of electronic voting systems in union elections.

However, since the types of technology in scope for the OLMS' RFI vary substantially—DRE-based voting, phone-based voting and remote voting over the internet—certain guidelines will be difficult to issue in a manner consistent with OLMS' duties to maintain voter secrecy, allow candidate observers and preserve records. Each of these technologies are at different states of maturity in government election administration and pose different sets of opportunities and complications with respect to issuing guidelines:

- **DRE-based voting:** DRE voting is wide-spread in government elections, and there is a large base of experience and guidelines from which to draw. For example, the U.S. Election Assistance Commission maintains the Voluntary Voting System Guidelines (VVSG)[4] which covers a number of administrative and substantive guidelines, including voting system functionality, usability/accessibility, hardware, software, telecommunications, security, quality assurance and configuration management. The VVSG is a large document, consisting of a set of requirements in one volume and administrative requirements for testing laboratories in a second volume. While not all of the elements of the VVSG may be applicable to union elections, the OLMS should certainly use the VVSG as a basis for its own guidelines and even consider using NIST's recommended overhaul of the VVSG, called the VVSG II,[5] which was developed from scratch by NIST and the EAC's Technical Guidelines Development Committee to better address the various existing types of voting systems and to incorporate state-of-the-art standards for the properties to which a voting system should be designed. ACCURATE has offered public comments at each revision stage of the development of the VVSG;[6] OLMS should take into account our commentary in that process into their guidelines.

- **Phone-based voting:** In government elections, phone-based voting is used mostly for accessibility accommodation, in only a handful of states,[7] and even where it is used, the method is much different from what the RFI describes as a pure phone-based interaction.[8] There are no guidelines in the VVSG for vote-by-phone systems and no such system has ever been certified for use

[4]The 2005 VVSG is the version currently in effect. *See:* U.S. Election Assistance Commission. *2005 Voluntary Voting System Guidelines*. Dec. 2005. URL: http://www.eac.gov/testing_and_certification/2005_vvsg.aspx

[5]U.S. Election Assistance Commission, 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.

[6]Aaron Burstein and Joseph Lorenzo Hall. *Public Comment on the Voluntary Voting System Guidelines, Version 1.1*. A Center for Correct, Usable, Reliable, Auditable and Transparent Elections (ACCURATE). Sept. 2009. URL: http://accurate-voting.org/wp-content/uploads/2009/09/ACCURATE-vvsgv11-final.pdf; Aaron Burstein and Joseph Lorenzo Hall. *Public Comment on the Voluntary Voting System Guidelines, Version II (First Round)*. A Center for Correct, Usable, Reliable, Auditable and Transparent Elections (ACCURATE). May 2008. URL: http://accurate-voting.org/wp-content/uploads/2008/05/accurate_vvsg2_comment_final.pdf; Erica Brand, Cecilia Walsh, Joseph Lorenzo Hall, and Deirdre K. Mulligan. *Public Comment on the 2005 Voluntary Voting System Guidelines*. A Center for Correct, Usable, Reliable, Auditable and Transparent Elections (ACCURATE). Sept. 2005. URL: http://accurate-voting.org/accurate/docs/2005_vvsg_comment.pdf.

[7]Connecticut, Maine, New Hampshire, Oklahoma, Vermont, and Puerto Rico. *See:* Verified Voting Foundation, Verifier Database query for IVS Inspire, http://www.verifiedvoting.org/verifier/searched.php?ec=allall&state=AS&vendor[]=IVS&submit=Search&rowspp=20000 (last visited, 14 March 2011).

[8]The product often used in government elections for accessible vote-by-phone is the IVS Inspire. This system allows a dedicated line from a polling place to call a server system in election headquarters where the voter can then listen to an audio ballot and indicate their selections using a familiar interface, the phone keypad. Depending on the implementation, the server

in federal elections by the EAC. The proposed VVSG II do have some minimal requirements[9] that would be applicable to vote-by-phone systems and NIST included "pure" vote-by-phone in a recent threat analysis of remote voting options.[10]

- **Remote internet voting:** As the RFI noted, remote voting over the internet in government elections has been limited to a number of special instances, often partisan primaries, and in each case it was never used again.[11] There are no guidelines available for remote internet voting and it is the consensus of technical experts that remote internet voting is highly risky for any election process that requires strong voter secrecy, auditability and voting free from undue influences such as coercion and vote-selling. We will save further discussion of the particulars for subsequent sections of this comment.

2. *Describe the potential advantages and disadvantages of electronic voting systems in union officer elections. For unions that have considered electronic voting systems, what factors guided your decision to either adopt or reject electronic voting systems?*

Advantages of electronic voting technologies include speed of tabulation, preventing overvotes and undervotes,[12] accommodation of voters with disabilities and language difficulty as well as greater flexibility with the physical location from which the voter chooses to cast their ballot.

Disadvantages include large numbers of security vulnerabilities, especially those useful for planting malicious code, but in the case of internet voting, vulnerability to denial-of-service attack, server penetration attack, and many types of insider manipulation and abuse. This is in addition to disadvantages associated with lack of observability, technology that has a much shorter life cycle, proprietary technology that can be difficult to prove will function properly, usability problems, and lack of voter verification leading to lack of auditability (meaningful recount capability).

3. *In elections other than union officer elections (for example, contract ratification votes, National Mediation Board elections, National Labor Relations Board elections, and national and local political elections), what are the voting system trends? Are there trends toward: (1) Electronic voting machines used for casting votes at polling sites; (2) electronic voting from remote site personal computers via the Internet; and (3) electronic voting from remote site telephones? How do these systems protect ballot secrecy and have these protections been effective?*

---

can either print a paper ballot at the server-end of the transaction (at elections HQ) or it provide a method for casting a marked ballot physically at the polling place. In the latter case, the server then faxes back the voted ballot information to the precinct system where the vote-by-phone terminal prints out a representation of the ballot. That paper ballot is then placed in the ballot box and counted by hand at the end of the day to add to the nominal voting system totals. (New Hampshire Assistant Secretary of State, Anthony Stevens, *personal communication*.)

[9] U.S. Election Assistance Commission, Technical Guidelines Development Committee, see n. 5, § 5.6.1-B, § 6.3.4.

[10] Andrew Regenscheid and Nelson Hastings. *A Threat Analysis on UOCAVA Voting Systems*. NISTIR 7551. National Institute of Standards and Technology, 2008. URL: `http://www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf`.

[11] Besides the cases of Alaska and Arizona in 2000 mentioned in the RFI, internet voting was used in several states—although concentrated in Florida—in the Federal Voting Assistance Project's VOI (Voting over the Internet) experiment in 2000, a precursor to the SERVE program (cited in the RFI), *see:* `http://www.fvap.gov/resources/media/voi.pdf`. We cannot cite a review article that discusses other instances, but we believe it has been used a number of other times in the following cases: by the Reform Party in its national primary in 2000, the Michigan-Democratic-Farmer-Labor party in a primary (we believe in 2004), by the Democratic Party to elect its overseas convention delegates in 2008, and by Okaloosa County, Florida in the 2008 general election. Most recently, it was used in 6 counties West Virginia in the 2010 general election to serve UOCAVA voters.

[12] An overvote is when a voter makes more choices than permitted for a given contest, invalidating their ballot for that contest. An undervote happens when a voter makes too few choices than the number permitted for a contest (of course, this can be on purpose where an overvote should not happen intentionally).

We are not familiar with the trends in this area.

4. *Are voter verified ballots and paper audit trails necessary safeguards for union officer elections? If so, why? If not, why not?*

The OLMS has a policy decision to make: Do union elections need to provide the ability to robustly audit election results and provide the capacity for a meaningful recount of disputed elections? If yes, then that has specific consequences for the technology: voter-verified ballots and paper audit trails are necessary. On the other hand, if union elections do not need to provide the capability for robust audits and meaningful recounts, then voter-verified ballots and paper audit trails are not necessary, but the outcome may be uncertain and subject to challenge. We are technologists and thus can advise about how to ensure that the technology achieves the OLMS's policy goals. However, we take no position on the policy question of whether union elections require robust audits and meaningful recounts.

Purely electronic records are vulnerable to silent, undetectable manipulation (or simply error) and VVPR with a required auditing process is the only available technology to guard against these dangers. To the extent that union officer elections need to be subject to robust audit processes and provide the capability for meaningful recounts, voter verified paper records (VVPR) must be produced by the system, adequately protected after ballot casting and subject to an audit process that is designed to manually count ballots to detect errors that would result in an incorrect election outcome. Election technologies that do not produce and retain a VVPR—such as DRE systems without VVPR, remote internet voting without VVPR and "pure" vote-by-phone without VVPR—cannot provide for meaningful recounts. Instead, these technologies are only capable of reporting the election totals as they exist in digital memory and then re-tallying the electronic records. That is, these systems cannot work to re-tally ballots from indelible records that voters have confirmed as representing their intent before they cast their ballots. Since no such record is produced and retained by these systems, auditors cannot statistically examine primary records (like VVPRs) in order to assess 1) the extent to which the voting technology has accurately recorded voter intent and 2) if the election outcome reported by the system is incorrect.

One of the complications in government elections is that it can be difficult and even impossible to run an election over, in the case that the system fails or is corrupted.[13] We are not familiar with the costs or legal implications of "do-overs" in union officer elections. However, even if it were possible to hold an inconclusive election again, the result would not necessarily be the same given the variation in environment, voter attention and other factors. That being said, it seems wise to only redo elections in extreme cases, where there is no other option and all effort has been made to ensure that the first election was run in a robust and auditable manner.

5. *If an electronic voting system has no voter verified paper ballots, how could a voter confirm that his or her vote was recorded accurately on the electronic ballot and stored accurately in the computer memory? Does the electronic display shown to the voter of the votes cast necessarily mean that the votes are stored or tallied as displayed?*

A voter cannot confirm that her vote was recorded correctly and stored accurately in electronic or digital storage. There is no currently available product that provides the ability for a voter to confirm that their vote was recorded and stored electronically; *i.e.*, that would allow a voter to visually verify that a representation of information on a display screen is appropriately stored in digital storage. There is active research into future technology that might provide such a capacity, using recent research results on

[13] Jack Maskell. *Postponement and Rescheduling of Elections to Federal Office*. Congressional Research Service. Oct. 2004. URL: `http://www.fas.org/sgp/crs/RL32623.pdf`, at 1.

cryptographic end-to-end voting systems.[14] However, such systems have only rarely been demonstrated in elections for public office, to our knowledge they are not currently available in the commercial market, and more research is needed on the extent to which those kinds of systems are usable for voters.

6. *If an electronic voting system has no voter verified paper ballots, can an observable recount be conducted? If so, how would this be accomplished?*

No meaningful recount or meaningfully observable recount can be conducted with an electronic voting system without voter-verified ballots and paper audit trails.[15]

An "observable" electronic recount can be conducted on a system without a VVPR, but the process consists essentially of the system operator clicking a "tabulate" button or pressing the "Return" key on the system keyboard to instruct the system to re-tally the votes. However, this process does not provide a meaningful, independent recount; if the original count was incorrect, then the electronic "recount" will be incorrect as well. In particular, if the votes were recorded incorrectly or were corrupted before they were counted, then an electronic recount will provide consistently incorrect results. Therefore, re-tallying the votes by an electronic recount process does not provide additional assurance in the correctness of the vote counts, nor does it provide a way to resolve disputes or respond to challenges to the integrity of the election.

Unfortunately, without voter-verified paper records, there is no way to conduct a meaningful, independent recount. While it is possible for a voting system to print out "Cast Vote Records" (CVRs)—in other words, to print out a representation of the cast ballots stored electronically by the system—this does not provide a meaningful recount capacity, because there is no assurance that the printed CVRs do, in fact, represent the ballots that were cast on election day. Further, voting systems are prone to usability errors where a mark made by a voter may be interpreted incorrectly by the system, and electronic recounts do nothing to address, detect, or correct these errors. This is why *primary* records of ballots—that is, ballot records that voters have marked themselves or have had the opportunity to confirm before casting—are the only records that lend themselves to *meaningful* recounts, where the best representations of voters' intents are tallied to arrive at results independent of the software and hardware of the system.

7. *If the electronic balloting system includes a function that prints paper versions of electronically stored ballots, but individual paper ballots are not voter-verified, does this function allow for a meaningful recount? Would these non-voter-verified paper ballots produced by the electronic system be independent of the electronic votes stored in the electronic system?*

No, this system does not allow for a meaningful recount.[16] There is no assurance that the non-voter-verified paper ballots (NVVPBs) produced by such a system match the votes that the voters cast. If there is an error in the electronic vote records, then that error will be blindly propagated to the NVVPBs, so printing out NVVPBs and counting them manually has little or no benefit. Consequently, manually counting NVVPBs does not provide a meaningful recount.

[14] Ben Adida. "Helios: web-based open-audit voting". In: *Proceedings of the 17th USENIX Security Symposium*. 2008. 335–348. URL: `http://www.usenix.org/event/sec08/tech/full_papers/adida/adida.pdf`; R. Carback, D. Chaum, J. Clark, J. Conway, A. Essex, P. S Herrnson, T. Mayberry, S. Popoveniuc, R. L Rivest, E. Shen, et al. "Scantegrity II municipal election at Takoma Park: the first E2E binding governmental election with ballot privacy". In: *Proceedings of the 19th USENIX Security Symposium*. 2010. 19–35. URL: `http://www.usenix.org/events/sec10/tech/full_papers/Carback.pdf`.

[15] We note that some cryptographic voting systems allow for meaningful recounts using purely electronic records. However, this requires the voter and observers to delegate their understanding of the system to cryptography experts. That is, these systems are *mathematically* verifiable but not necessarily *humanly* verifiable.

[16] Our answer to Question 6 discusses at length the issue of meaningful recounts.

The NVVPBs produced by such a system are not independent of the electronic vote records. The NVVPBs are a direct copy of the electronic vote records, produced automatically and without human involvement, and as such inherit any errors that may be present in the electronic vote records.

8. *Are there technologies or systems that provide a check on the accuracy of the electronic system that is independent of the software in the system? If so, what are those technologies or systems?*

VVPRs that are checked by the voter and stored securely coupled with a "risk-limiting audit" process[17] are the most reliable methods for providing a check on the accuracy of the electronic system that is independent of the software of the system.[18]

Cryptographic voting protocols and systems, while not ready for use in critical elections and currently at the research-prototype stage of maturity, hold considerable promise for removing the physical record requirement from the voter-verification record. Please see the associated discussion and references in our response to Question 5, above.

9. *How can observers participate meaningfully in all phases of the election process in an electronic voting system environment? How can remote site electronic voting systems ensure that candidates have the right to observe all aspects of the election? Are there features of electronic voting systems that establish or replicate processes for candidates to have observers at the polls and at the counting of the ballots? If so, what are those features?*

There are no processes or features in electronic voting systems that would allow observers to observe the digital counting of ballots. Observability requires VVPRs that are physically transported and stored with chain of custody records and two-person custody protocols[19] where union members have the right to follow the ballots physically during transport and then physically watch the audit process or recount.

10. *Most remote site electronic voting systems use a voter identification number (VIN) for each voter to log into the system and vote. In these systems, what safeguards exist to prevent the connection of a voter's identifying information and his or her vote?*

To best assure that a voter's identity could not be linked to their ballot data, systems that use a VIN must completely disassociate the VIN from ballot data after the ballot has been received and it is ascertained that the ballot was legally cast by a legal voter who has not already voted.[20]

[17] "Risk-limiting" audits are designed to count as few VVPRs as needed to achieve a pre-set level of confidence that a full hand count would not differ from the outcome reported by the voting system, or the method "escalates" to count all VVPRs in a full hand tally. For a thorough discussion of "risk-limiting" audits, see Hall *et al.*: Joseph Lorenzo Hall, Luke W. Miratrix, Philip B. Stark, Melvin Briones, Elaine Ginnold, Freddie Oakley, Martin Peaden, Gail Pellerin, Tom Stanionis, and Tricia Webber. "Implementing Risk-Limiting Post-Election Audits in California". *Electronic Voting Techology Workshop/Workshop on Trustworthy Elections 2009 (EVT/WOTE 2009)* (Aug. 2009). URL: `http://www.usenix.org/events/evtwote09/tech/full_papers/hall.pdf`.

[18] Software independence is defined and discussed in Rivest and Wack: Ronald L. Rivest and John Wack. *On the Notion of "Software Independence" in Voting Systems*. National Institute of Standards and Technology HAVA Technical Guidelines Development Committee. July 2006. URL: `http://vote.nist.gov/SI-in-voting.pdf`.

[19] Two-person custody protocols require sensitive materials to always be transported and/or under the control of two independent parties or officials, ideally with different partisan/union affiliations.

[20] For completeness, we note two other options, only one of which appears to meet the OLMS' criteria. In the United Kingdom, election officials maintain a secure mapping between voter-identifiable numbers (like VINs) and ballots. This record is kept as a state secret, requiring a Court to unseal this mapping and then only in cases where fraud can be clearly shown and the mapping is needed to prosecute the offenders or attempt to exclude erroneous ballots from the tally. However, such a secure mapping could be used to identify a voter and their ballot, so this does not meet the legal requirements for ballot secrecy as outlined in the RFI. (The RFI describes how the Courts have interpreted the controlling statute, Title IV of the

11. *Some systems separate the VINs from the particular voted electronic ballots so that one individual or server controls access to the VINs and a separate individual or server controls access to the voted electronic ballots. In those systems, can the voter and the vote be reconnected? How can voters have confidence that there is no connection of voter and vote and that their votes remain secret?*

There is no way to prove that the VIN cannot be re-associated with the voter's ballot, or that a copy of the association was not surreptitiously saved by an adversary. At this point, there is no choice but to trust the integrity of the officials administering the election.

We do not know whether any particular system for union elections achieves ballot secrecy. Determining whether any particular system achieves ballot secrecy requires more than knowing the general approach the system takes; it requires careful analysis of the details of the design and implementation of the system by a qualified technical expert. Without analyzing a specific situation, in the context which it is intended to be used, it is not possible to state whether it provides ballot secrecy.

Generally speaking, if the association between VIN and ballot data is destroyed, only a few methods remain that we know of to re-establish that connection, and each require the voter to cooperate; *i.e.*, the voter must want to prove how they voted.[21]

One way that voters can have confidence that their votes will remain secret is for some independent agency to carefully assess the system to determine whether it achieves the ballot secrecy goals, and then certify their results. If voters trust in the competence, independence, and integrity of that agency, then this might provide voters confidence that there is no way to determine how any particular individual has voted. Another approach to build confidence is for the developer of the voting system to disclose the design, implementation, and source code of the voting system to the public for purposes of analysis, to allow qualified experts to do their own analysis of its provisions for ballot secrecy.

12. *Is there a software protocol that can restrict the transfer of any information that could potentially link a voter to his or her vote? If there is such a software protocol, can it be re- programmed to permit the link? Can such re-programming be detected afterward?*

There exists no such software protocol that we know of.[22]

Labor-Management Reporting and Disclosure Act (LMRDA), as requiring the union to provide strict ballot secrecy in both the act of elections and post-election procedures (76 Fed. Reg. 1561).)

Another, very technical, solution may exist in the use of "mix-net encryption", where the identity of the voter is connected to an encrypted ballot (where the contents of the ballot cannot be deciphered without a special key). After each ballot is validated as being a legal ballot from a legal voter, the voter's identity is disassociated from the ballot, the ballots are then subject to a complex encryption, shuffling and decryption process before they are tallied. For an approachable tutorial on the use of cryptography in elections, please see Ben Adida's presentation, "Cryptography and Voting", `http://www.slideshare.net/benadida/cryptography-and-voting`.

[21] If the voter wants to prove how the voted to a third-party or election official, there are two well-known methods that are difficult to protect against. First, if the voting system allows write-in voting, the voter can write-in a special name or series of characters that, if associated with the rest of their ballot choices, can identify that ballot record as theirs. To protect against this, write-in candidates should be required to qualify to run as a write-in candidate, applying up to a week before the relevant election. And only votes for qualified write-in candidates should be publicly reported, and never associated with the rest of the ballot choices on these ballots.

In addition, a voter can use a special pattern of votes on their ballot to identify their ballot. A voter would make the choice on their ballot that the third-party asked of them, and then fill out a distinctive pattern for the remainder of the ballot. If this pattern only exists in one ballot and all ballots are reported publicly, the third-party can check to make sure this special ballot exists in the list of tallied ballots and know their collaborating voter voted in the manner they asked. However, if there are only a few choices per ballot, this method becomes much less powerful. That is, if there is no possibility for a "distinctive" ballot, voters and third parties can't use this method to collude. We suspect union officer election ballots only have a few choices, so this may not be a relevant concern.

[22] Even if the VINs are completely discarded, pattern voting attacks and the write-in text attacks could still be used by a voter to identify their ballot. Please see the discussion in n. 21.

13. *In a remote site electronic voting system, if a determination is made that a voter is ineligible after he/she has already voted, can that vote be removed from the system without reconnecting the voter and vote? If not, can an observer challenge a voter's eligibility after voting has begun or must all such challenges be made prior to balloting?*

If the voter's identity (VIN) is completely disassociated from their ballot, there should be no way to identify their ballot and, no, there would be no way to remove the ballot from the system. In such a system, all verification of a voter's legal status and possible challenges should take place before the ballot is cast.

If the ballot is linked to the voter even after it has been cast, it would be possible to find the ballot and remove it from the system. However, unless the system is using a cryptographic voting protocol, where the voter's choices are obfuscated when the ballot is submitted, there remains a very real possibility that the voter's identity and ballot contents could be ascertained, and this would not meet the requirements specified by OLMS.[23]

14. *How does a remote site electronic voting system deal with a "spoiled" ballot situation, i.e., when a member marks and submits a ballot in error, such as failing to vote for a particular race? Can that ballot be identified and voided and can that member be allowed to vote again? How does the system accomplish this without reconnecting the voter and vote?*

Please see our answer to Question 10. The ability to filter out ineligible votes or instances of multiple voting is the reason the dissociation between VIN and ballot must not be done until *after* the legality of the ballot has been validated.

15. *In a remote site telephone voting system, can the system log and store the caller/voter's telephone number as well as the caller/voter's VIN and voting data?*

Certainly, a vote-by-phone system can record the reported Caller ID number for the incoming call and associate it with the voter's VIN and ballot data. Of course, if two or more union members live at the same household they will have the same phone number; in this case, relying on the number reported by Caller ID won't work to authenticate or disambiguate them. If Caller ID information is recorded together with the voter's votes, then it could be used to connect a voter to his/her votes, potentially endangering voter privacy. We caution against use of Caller ID information to authenticate voters or verify that the caller is eligible to vote. Caller ID information can be readily faked.

In general, there are two methods one can use to identify a caller: Caller ID and Automatic Number Identification (ANI). These two methods have different characteristics.

Caller ID conveys the caller's phone number and name, according to the company or phone switch that originated the call. Caller ID provides the functionality we are familiar with, where when someone calls us, we can see the name and number of who is calling us. Unfortunately, Caller ID can be easily spoofed: a malicious individual can easily place a call and arrange to have the Caller ID information contain any information he chooses (including the information for some other person). There are commercial services that are readily available to the public which make it easy to place a call with fake or forged Caller ID information.[24] There are even apps for iPhone, Blackberry, and Android phones that can be used to place calls with a spoofed Caller ID.[25] Caller ID spoofing has been used to place prank calls, including several widely publicized incidents.[26] As a result, making calls with forged caller ID

[23] 76 Fed. Reg. 1561.

[24] *See*, *e.g.*, SpoofCard, SpoofTel, PhoneGangster, StealthCard, BluffMyCall, Itellas for examples of such services.

[25] *See*, *e.g.*, SpoofApp.

[26] See the following Wikipedia entry for examples of Caller ID spoofing incidents: `https://secure.wikimedia.org/wikipedia/en/w/index.php?title=Caller_ID_spoofing&oldid=414741528` (last visited 14 March 2011).

information requires no technical expertise and has very little cost. Another problem with Caller ID is that phone subscribers have an option to block outgoing Caller ID; calls from such a phone number will not come with Caller ID information.

For calls placed to toll-free numbers, another way to identify the caller is through ANI. ANI information is used by phone companies for billing purposes and can be used by the recipient of the toll-free call to identify the caller. ANI is akin to Caller ID, in that it conveys the phone number of the party placing the caller. However, ANI is distinct and separate from Caller ID, and has different features. Because ANI is used for billing information, it cannot be easily spoofed or forged. There are no known ways to place a call with spoofed ANI information that are readily available to the public, so ANI information provides better security than Caller ID. One disadvantage of ANI information is that it is restricted to calls to toll-free phone numbers. However, there are commercial services that capture ANI information for calls to other phone numbers, for a fee;[27] these services work by forwarding the call to a toll-fee number and then back to the intended recipient.

For these reasons, we do not recommend use of Caller ID to authenticate voters. If voting systems wish to identify the caller's phone number and use this to authenticate the voter, we recommend that they use ANI information, as ANI information is harder to spoof.

16. *What safeguards exist to prevent malicious or fraudulent software (e.g., software that would delete or change vote totals) from being embedded in an Internet voting system? If such code was introduced or embedded, would it be possible to detect? If so, how? How would an allegation of software tampering be resolved? If electronic voting system software is proprietary, would a third party, such as OLMS, be allowed to inspect the software to resolve an allegation of tampering? If so, how? How would a third party, such as OLMS, be allowed access to the proprietary software codes to resolve the allegation of tampering?*

In an election with robust auditing (or recounts) based on VVPRs, it does not matter if there are bugs in the software, or malicious code, or if fraudulent software has been substituted in place of the "real" software. The auditing or recount process will detect and correct the election totals, and an investigation of the software problems can proceed after the fact while officials still confidently certify the (audited) results of the election.

Only limited safeguards against malicious and/or fraudulent software exist. Such protections are as difficult as ensuring any arbitrary software has no malicious code, and this is a long and active area of research in computer science. Assuming software can be developed without flaws or backdoors (which we do not know how to do), protecting the software subsequently requires a "chain of custody" from the original source code through to the built binaries (the executables compiled from the source code) to the software ultimately loaded on voting machines. Cryptographic digital signature technology is one component of this process, but there is no practical system in place today that can solve each part of this problem, and even implementing digital signatures requires careful attention to chain of custody and a high-degree of technical sophistication. Source code review by independent experts can help to detect poor programming practices, but cannot assure that code is free of bugs or malicious code. A "trusted build" process that uses this reviewed code to build executables is useful, but it is very difficult to discern whether or not the "trusted" software is ultimately resident on a voting machine in the field.

Unfortunately, detecting all malicious and/or fraudulent code in a standard set of voting system software is impossible. Experiments have shown that even expert review is insufficient. A study by Ping Yee of a very simple prototype voting system with deliberately installed flaws showed that expert reviewers (including ACCURATE PIs) were unable to detect vulnerabilities, even when told they were

[27] *See*, *e.g.*, TrapCall.

present.[28] Other studies have shown that deliberately installed "backdoors" installed by insiders can go years before detection.

The best way to resolve allegations of software tampering is to conduct a meaningful audit or recount of the election results, by auditing or recounting voter-verified paper records. Source code disclosure could also play a role, but it has major limitations and is unlikely to be a fully satisfactory answer to allegations of software fraud.

Assuming the source code for the voting system is not open source or disclosed source software, for OLMS to be able to gain access to source code, unions must specify in their contracts with election vendors that they require all relevant source code, documentation and "build tools" to be deposited in escrow with a software escrow facility and that OLMS be listed explicitly as a software escrow beneficiary. This agreement should specify that the source code be released to OLMS if certain "triggers" are reached, such as a finding that source code is needed to help resolve allegations of tampering. An alternative to escrow would have OLMS require that vendors agree to provide source code to qualified experts at OLMS' request or agree to provide source code to the public upon request. OLMS could take possession of the source code and itself provide access to experts or members of the public, but vendors will probably argue that they need very stringent protection of code and materials.

To gain access to the source code, the escrow facility would have to give OLMS the source code, OLMS would then have to establish a secure facility for the analysis and then have any agents working on the investigation sign Non-Disclosure Agreements.

17. *If OLMS receives an election complaint challenging the software code in an electronic voting system, how can OLMS ensure that the code examined by OLMS in the investigation is the same code that was in place and operational during the challenged election?*

There is no way to ensure that the escrowed software code is the same as that in place and operating during the election. Please see the discussion in our response to Question 16, as much of that discussion is relevant here.

To help ensure that executables running in the field are bona-fide copies of the trusted build executable, the Nevada Gaming Control Board performs random "field audits" of gaming devices where they plug in a device that can check the "fingerprint" (a cryptographic hash) of the software. Even this involved procedure is far from perfect: such audits have been thwarted in the past to both misreport the "fingerprint" of the software and to write malicious software onto the device.[29]

18. *In the electronic voting systems with which you are familiar, are all system activities of the union or third party election administrators permanently recorded or logged into the system? What safeguards exist to prevent accidental deletion from or tampering with the log? How could a third party, such as OLMS, investigate alleged tampering with the log? Does this log file, or other similar system file or database, include each voter's entry into the system, along with that voter's IP address, VIN, and voting data in sequential order?*

Systems and events mediated by the election system can be logged. Activities that do not take place in or through the system must be logged using external systems and procedures (*e.g.*, closed-circuit television, paper sign-in sheets, etc.) that are examined and audited. However, voting system logs are notoriously neither secure nor robust. For example, in response to a case in California where a voting

[28] Ka-Ping Yee. *Report on the Pvote Security Reviews*. UCB/EECS-2007-136. EECS Department, University of California, Berkeley, 2007. URL: `http://www.eecs.berkeley.edu/Pubs/TechRpts/2007/EECS-2007-136.html`.

[29] See the discussion by Burbank of the case of Ron Harris: Jeff Burbank. *License to Steal: Nevada's Gaming Control System in the Megaresort Age*. University of Nevada Press, 2005. ISBN: 0874176247, at 187.

system deleted vote data and did not log this event, ACCURATE PI David Wagner authored a report at the request of the California Secretary of State summarizing the state of the art in voting system logging.[30] We recommend OLMS study Wagner's report in detail.

Robust, tamper-evident logging is a topic of current research at ACCURATE and PI Dan Wallach and his research group have made important contributions in this field.[31] Suffice it to say that anything that is a challenging focus of current computer science research is a difficult problem that has not yet been solved by industry or yet made it into production systems.

To preserve ballot secrecy, voting system log files have to be carefully designed not to log ballot data or voter identities, as that would violate ballot secrecy. However, some data elements, such as precise time-stamps, are desirable for logging but can be problematic when combined with other data sources. Data external to the voting system and out of the control of administrators—for example, observations of the order of voters at a particular voting machine at the polling place—can be used with time-stamps to identify voters' ballots.

19. *What safeguards exist to prevent vote manipulation by "insiders" such as computer programmers, equipment manufacturers, technicians, system administrators, or election officials who may have legitimate access to election software and/or data? How could a third party, such as OLMS, investigate allegations of insider attacks?*

The optimal safeguard, again, is to rely on the *observability* of VVPRs, chain of custody and the audit (or recount) process. If these processes are carefully observed from beginning to end by interested parties, then it is much more difficult for insiders to manipulate the process without detection.

Certainly, standard personnel controls for security-critical systems, such as background checks and vendor compliance audits, as well as penalties for reports of misbehavior can help internalize defenses against insider threats. However, there is no absolute solution as the software vendor is *trusted* to build and deliver a product and perfect detection of vulnerabilities and malicious code is not possible.

One partial safeguard is through separation of duties: ensure that employees of the vendor who develops the software do not have any role in operations/conduct of the election (they should not run the election, they should not have access to the election equipment/systems during the election), and conversely, that those who operate the election equipment are not given access to change the software code. Employees of the vendor who develops the software are the ones in the best position to place backdoors or secret defects in the software, and in the best position to know the weaknesses of the system. Election officials with access to the equipment and who run the election are in the best position to activate or make illicit use of those backdoors or defects. By ensuring that no one individual is in a position to both introduce a backdoor and activate it, one can potentially make it harder for such attacks to occur.

20. *How would the use of electronic balloting affect the issue of voter intimidation, if at all? For any voter intimidation that might take place in the context of an election using electronic balloting, what safeguards have been or could be used to address the issue?*

Electronic balloting does not necessarily affect voter intimidation. What affects it is voting from an unsupervised environment—whether it be on paper (vote-by-mail) or electronically (remote internet voting). Voters are much less likely to be intimidated if they are guaranteed the ability to vote alone

[30] David Wagner. *Voting Systems Audit Log Study*. University of California, Berkeley commissioned by the California Secretary of State. June 2010. URL: `http://www.cs.berkeley.edu/~daw/papers/auditlog-ca10.pdf`.

[31] Scott A. Crosby and Dan S. Wallach. "Efficient Data Structures for Tamper-Evident Logging". In: *Proceedings of the 18th USENIX Security Symposium*. 2009. 317–334. URL: `http://www.usenix.org/events/sec09/tech/full_papers/crosby.pdf`.

in a voting booth. This requires polling places and well-trained poll workers who have the mandate to remove individuals that may be attempting to coerce or influence voters. Unfortunately, civic elections rely on special election laws to prevent certain activities in a polling place; we are uncertain how union election sites might achieve the same protections. Perhaps one answer is to use trespass laws where only people who agree to a set of conditions are allowed on the premises of a union polling place and if they intimidate voters or solicit voters to buy votes, they can be removed from the site.

One way that electronic balloting can possibly mitigate voter intimidation is to allow voters to vote as many times as they like, and only count the last vote.[32] This has important limitations, but may provide some voters who are intimidated with a way to respond, in some situations.

Careful attention to honest dissociation of VINs from ballots is critical to preventing voter intimidation in systems that connect a VIN to ballot data before allowing a ballot to be cast and disassociating the two. Maintaining links between voter identities and ballot data is a weakness with respect to intimidation, regardless.

21. *What safeguards exist to prevent denial of service attacks, "spoofing" (i.e., when one person masquerades as another and gains illegitimate access), automated vote buying, and viral attacks on voter personal computers? How could a third party, such as OLMS, investigate allegations of such activity?*

Combating denial of service (DoS) requires either (or both) long-term availability—voting over a number of days or weeks—or dynamic availability—putting resources in place as demand increases (regardless of whether or not that demand is real or part of the DoS attack). Filtering out the source of a DoS attack can be effective; however, often DoS attacks are distributed (DDoS), in which case identifying DoS sources and filtering them out may take resources away from availability strategies.

Spoofing resistance requires reasonable authentication.[33]

The most practical safeguard against automated vote-buying is to require supervised kiosks for voting, such that vote-buying becomes a "retail" endeavor with some likelihood of detection by poll workers. Otherwise, there will be no defense other than hoping to receive tips that buying is occurring and locating the buyer or buyer's server before a detrimental amount of votes have been bought. Again, a key protection against vote-buying is honest and complete dissociation of VINs from ballots, or never having this information in the first place. Regarding tips of vote-buying, perhaps OLMS could set up an anonymous whistleblower hotline where concerned individuals can anonymously report incidents of vote-buying. OLMS could use this to monitor reports of vote-buying and target investigation as appropriate.

Regarding viruses, there is little OLMS can do to further protect voters' personal computers from malware. This problem is difficult and completely beyond the control of OLMS or the union. Voters will need to use virus scanners to protect against known strains of malware and, even more challenging, learn and employ proper security hygiene and discipline with the use of the computer on which they plan to vote. We cannot emphasize enough how hard of a problem this is, and how this aspect of the remote internet voting problem by itself should counsel OLMS to not allow voting on platforms out of the control of election authorities.

The best way to investigate allegations of these kinds of activities would be to conduct a meaningful audit or recount of the voter-verified records, if possible, and hire technically qualified experts to conduct an investigation. Unfortunately, investigating many of these allegations will likely require specialized technical expertise in fields such as computer security, computer science, or forensics.

[32] The design of public elections in Estonia utilize this strategy.

[33] See the discussion in the NIST Threat Analysis work for further discussion. (Regenscheid and Hastings, see n. 10)

22. *There are reported cases of electronic voting system malfunctions in civic elections where votes have either not been recorded or have not been recorded accurately. These cases include: Volusia County, Florida (2000), Broward County, Florida (2004), Franklin County, Ohio (2004), Sarpy County, Nebraska (2004), Carteret County, North Carolina (2004), and Sarasota County, Florida (2006). What safeguards exist to detect such malfunctions? How could a third party, such as OLMS, investigate allegations that such malfunctions occurred?*

Robust audits (or recount) from chain-or-custody-protected VVPR records is the best safeguard against malfunction. There is no other strong protection against bugs, malicious code, or insider error or fraud. In addition, voters do not always check the VVPR before casting,[34] so some education that voters must check the VVPR record before casting their ballots would be helpful.

Poll-workers should be well-trained to implement chain of custody procedures with VVPRs and other sensitive records and the election authority should audit these procedures to assess the extent to which they are being followed. OLMS will need to ensure that each of these is happening properly and with minimal error. Reports of malfunction from unions, third party administrators and voters should be taken seriously and investigated.

23. *What safeguards exist to prevent "phishing" in remote Internet voting systems? "Phishing" is a scheme that uses a web page set up to look just like the union's voting web page. Union members are brought to the site by email, links, or reminders to vote with an embedded link. The union member "votes" on the fake site. The person who sets up the fake site then has the voter's VIN and other identifying information which the person then uses to log onto the real site and vote in place of the real voter. How could a third party, such as OLMS, investigate allegations of phishing?*

Phishing (URL spoofing) is a challenging threat for uncontrolled internet voting systems. These systems will need to employ Secure Sockets Layer (SSL)/Transport Layer Security (TLS) encryption to authenticate themselves to voters and provide encryption of traffic between the system and the voter's computing device. However, studies have shown SSL/TLS to be very limited in its effectiveness at defeating phishing: phishers can easily set up a non-SSL web site that looks like the real one, and many users will not notice.[35] One limited defense against phishing attacks is to require the use of SSL/TLS sitewide, across the entire site, not just for the password, which would reduce the ability for malicious parties to hijack or redirect a user's session. However, we must emphasize that defenses against phishing attacks are far from fool-proof and this remains a hard problem and an active research topic in web security.

Phishing is not the only web-based attack with which OLMS should be concerned. Cross-site scripting (XSS), Cross-site Request Forgery (XSRF), social-engineering phishing attacks ("spear-phishing") and many other web security attacks are all relevant. A complete review of web security vulnerabilities and the extent to which these can be mitigated against is beyond the scope of this public comment.

24. *Are there any other potential issues with the legality or practicality of electronic voting systems that have not been addressed in the preceding questions? If so, please explain.*

There are a number of potential issues that OLMS' questions did not address:

[34] Bryan A. Campbell and Michael D. Byrne. "Now Do Voters Notice Review Screen Anomalies? A Look at Voting System Usability". In: *Electronic Voting Techology Workshop/Workshop on Trustworthy Elections 2009 (EVT/WOTE 2009)*. 2009. URL: `http://www.usenix.org/events/evtwote09/tech/full_papers/campbell.pdf`.

[35] R. Dhamija, J. D Tygar, and M. Hearst. "Why phishing works". In: *Proceedings of the SIGCHI conference on Human Factors in computing systems*. 2006. 581–590.

- Both the servers used to conduct remote internet voting as well as the network on which the vendor develops voting system software will be subject to attack over time. The resistance of the software and voting system will depend on how well these systems can be protected. Considering the frequency of attacks and successful penetrations on U.S. military and corporate information systems, OLMS will want some evidence from election administrators and vendors that they are vigilant in their computer and network security controls and deal appropriately with any network penetrations.

- Certain methods of transmitting voted ballots are just as problematic as internet transmission, although they may seem benign at first blush. Email is not, in any sense of the word, inherently secure. Voted ballot data should not be sent via email. For different reasons, we also advise against using PDF as a electronic ballot medium. PDFs can contain arbitrary code and PDF readers are a frequent source of critical security vulnerabilities.

- One idea that might work for union elections is to require vendor warranties on software they provide for voting. That is, if a vendor is willing to warranty their software product against vulnerabilities that could be exploited to manipulate an election, this may provide a powerful incentive for diligence in software development. It could also provide a financial recourse useful for conducting an election over again if an election's outcome cannot be determined due to error or fraud as a result of voting system flaws.

- Finally, there are serious supply chain issues that are not easily tractable. Few voting systems are developed entirely by one vendor; most have software and hardware that are amalgamations of various vendors' products. It makes sense for OLMS to have insight and investigatory leverage over these vendors so that any potential party that might seek to discredit a union election can be subject to OLMS scrutiny.

3 Conclusion

ACCURATE appreciates the opportunity to comment on OLMS' effort to provide guidelines for electronic voting in union officer elections. Electronic voting is extremely difficult to assure with any confidence. ACCURATE recommends that chain-of-custody-controlled voter-verified paper records (VVPRs) be required for voting systems involved with critical elections. Further, VVPRs are not much of a safeguard without audit processes that serve as a check on the voting system, ensuring that the reported election outcome is correct. We strongly urge the Department of Labor to not allow internet voting in the resulting guidelines, as there simply are no effective, comprehensive methods for ensuring ballot secrecy and/or system integrity and reliability.

We offer our analysis, experience and expertise in the hope it will help OLMS develop responsible and technically-informed guidelines for electronic voting. We would be happy to answer any questions OLMS has about our comments and engage in further dialog with OLMS, unions, vendors or technical experts.