<PRORULE>

<PREAMB>

DEPARTMENT OF LABOR

Office of Labor-Management Standards

29 CFR Part 452

RIN 1215-AB84

RIN 1245-AA04

Guidelines for the Use of Electronic Voting Systems in Union Officer Elections

AGENCY: Office of Labor-Management Standards, United States Department of Labor.

ACTION: Request for information from the public.

SUMMARY: This notice is a request for information from the public to assist the Department of Labor ("Department") in issuing guidelines concerning the use of electronic voting systems in union officer elections. "Electronic voting systems" is meant to include: electronic voting machines used for casting votes at polling sites; electronic voting from remote site personal computers via the Internet; and electronic voting from remote site telephones. "Electronic voting systems" is not meant to include electronic tabulation systems where votes are cast non-electronically but counted electronically (such as punch card voting or optical scanning systems). Title IV of the Labor-Management Reporting and Disclosure Act of 1959 ("LMRDA") establishes democratic standards for the conduct of union officer elections. The LMRDA does not, however, require a particular method or system of voting. Labor organizations are free to establish their own methods or systems of voting for officer elections as long as they are consistent with lawful provisions in the union's constitution and bylaws and the provisions of

Title IV of the LMRDA. Labor organizations and other interested parties have sought guidance from the Department regarding the LMRDA compliance of electronic voting systems. This request for information seeks public comment to assist the Department in the consideration and issuance of such guidance.

DATES: Comments must be received on or before [**INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER**].

ADDRESSES: You may submit comments, identified by RIN 1215-AB84 and 1245-AA04. (The Regulatory Information Number (RIN) identified for this rulemaking changed with the publication of the Spring 2010 Regulatory Agenda due to an organizational restructuring. The old RIN (1215-AB84) was assigned to the Employment Standards Administration, which no longer exists; a new RIN (1245-AA04) has been assigned to the Office of Labor-Management Standards.) The comments can be submitted only by the following methods:

Internet: Federal eRulemaking Portal. Electronic comments may be submitted through *http://www.regulations.gov*. To locate the proposed rule, use RIN 1245-AA04 or RIN 1215-AB84. Follow the instructions for submitting comments.

Delivery: Comments should be sent to Stephen J. Willertz, Director of the Office of Enforcement and International Union Audits, Office of Labor-Management Standards, U.S. Department of Labor, 200 Constitution Avenue, N.W., Room N-5119, Washington, DC 20210. Because of security precautions, the Department continues to experience delays in U.S. mail

delivery. Commenters should take this into consideration when preparing to meet the deadline for submitting comments.

Comments will be available for public inspection at *http://www.regulations.gov*, and during normal business hours at the above address.

FOR FURTHER INFORMATION CONTACT: Stephen J. Willertz, Director of the Office of Enforcement and International Union Audits, Office of Labor-Management Standards, U.S. Department of Labor, 200 Constitution Avenue, N.W., Room N-5119, Washington, DC 20210, olms-public@dol.gov, (202) 693-1182 (this is not a toll-free number). Individuals with hearing impairments may call 1-800-877-8339 (TTY/TDD).

SUPPLEMENTARY INFORMATION:

The purpose of this request for information is to seek public comment on the use of electronic voting systems in union officer elections. The comments from interested parties, including unions, union members, union officers, technology experts, academics, election service providers, public interest groups, and the public will help the Department issue guidelines in describing minimum standards that electronic voting systems must meet to comply with the provisions of LMRDA Title IV. In addition, the comments should help determine what issues should be addressed and what specific standards should be included in the guidelines. These guidelines and standards are intended to assist the Department in its obligation to ensure compliance with LMRDA Title IV.

I. Background

A. Description of Electronic Voting Systems

The following are general descriptions of the three basic types of electronic voting systems that OLMS has encountered. They are not all-inclusive definitions of all electronic voting systems.

(1) Electronic voting machines used for casting votes at polling sites.

This is a direct-recording electronic (DRE) voting system in which voters mark their votes directly into an electronic device at a predetermined location monitored by election officials. The system records votes by means of a ballot display provided with mechanical or electro-optical components that can be activated by the voter (typically by buttons or a touchscreen). It is a computer-based voting system, running configured software, using computer voting stations, terminals, or kiosks that are set up in a securable location or locations. Voters must come to a predetermined location where they are first authenticated as eligible voters, and then vote at a computer terminal. Voting data is stored by the electronic device on a computer hard disk or a portable diskette, CD-ROM or smartcard. The system keeps an electronic record and may also keep a paper record, which may be verifiable by the voter, enabling a post-election audit. The system may also provide a means for transmitting individual ballots or vote totals to a central location (on either removable portable devices, such as diskettes, or by a computer network) in order to consolidate and report results at the central location. The system, as described here, is not a Web-based Internet voting system.

(2) Electronic voting from remote site personal computers via the Internet.

This is a DRE voting system that is Web-based in which voters do not have to vote from a predetermined location. Instead, they can register and vote from any Internet-connected personal computer (PC) or other mobile electronic device anywhere in the world. Voters connect to a

central server using a standard Internet browser. Both registration and voting are accomplished through the Web interface. This system uses a voter identification number (VIN) for each voter to log into the system and vote. Some such systems then 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.

(3) Electronic voting from remote site telephones.

This is a DRE voting system in which voters register and vote from remote site telephones. They do not have to vote at any specific predetermined location. Voters identify themselves with voter identification numbers (VINs) and record their votes directly into a computer system using the key pads on their telephones, by following a series of recorded instructions. Voters call a predetermined telephone number and respond to verbal prompts given by the system. Using the phone keypad, the voter enters choices. The computer system records those choices as votes.

B. Statutory, Regulatory and Administrative Framework

Title IV of the LMRDA, 29 U.S.C. 481-484, and interpretive regulations issued by the Department, 29 CFR Part 452, establish standards for the conduct of union officer elections, including minimum standards for:

- Voter secrecy
- Candidate observer rights and election safeguards

- Preservation of records

Voter Secrecy

LMRDA Section 3(k), defines a secret ballot as: "the expression by ballot, voting machine, or otherwise, but in no event by proxy, of a choice with respect to any election or vote taken upon any matter, which is cast in such a manner that the person expressing such choice cannot be identified with the choice expressed." 29 U.S.C. 402(k). Section 401(a) requires that "every national or international labor organization… shall elect its national officers…by secret ballot among the members in good standing or at a convention of delegates chosen by secret ballot." 29 U.S.C. 481(a). Section 401(b) requires that "every local labor organization shall elect its officers… by secret ballot." 29 U.S.C. 481(b). Section 401(d) requires that "officers of intermediate bodies… shall be elected… by secret ballot among the members in good standing or by labor organization officers representative of such members who have been elected by secret ballot." 29 U.S.C. 481(d).

The Department's regulations at 29 CFR 452.97 state that a prime requisite of elections regulated by title IV is that they be held by secret ballot among the members or in appropriate cases by representatives who themselves have been elected by secret ballot among the members. A secret ballot under the Act is "the expression by ballot, voting machine, or otherwise, but in no event by proxy, of a choice. . . cast in such a manner that the person expressing such choice cannot be identified with the choice expressed." Secrecy may be assured by the use of voting machines, or, if paper ballots are used, by providing voting booths, partitions, or other physical arrangements

permitting privacy for the voter while he is marking his ballot. The ballot must not contain any markings which upon examination would enable one to identify it with the voter. Balloting by mail presents special problems in assuring secrecy. Although no particular method of assuring such secrecy is prescribed, secrecy may be assured by the use of a double envelope system for return of the voted ballots with the necessary voter identification appearing only on the outer envelope.

In addition, should any voters be challenged as they are casting their ballots, there should be some means of setting aside the challenged ballots until a decision regarding their validity is reached without compromising the secrecy requirement. For example, each such ballot might be placed in an envelope with the voter's name on the outside. Of course, it would be a violation of the secrecy requirement to open these envelopes and count the ballots one at a time in such a way that each vote could be identified with a voter.

Candidate observer rights and election safeguards

Section 401(c) of the LMRDA requires that "adequate safeguards to insure a fair election shall be provided, including the right of any candidate to have an observer at the polls and at the counting of the ballots." 29 U.S.C. 481(c).

The Department's regulations at 29 CFR 452.107(a) state that under the provisions of section 401(c), each candidate must be permitted to have an observer (1) at the polls and (2) at the counting of the ballots. The right encompasses every phase and level of the counting and

tallying process, including the counting and tallying of the ballots and the totaling, recording, and reporting of the tally sheets. If there is more than one polling place, the candidate may have an observer at each location. If ballots are being counted at more than one location or at more than one table at a single location, a candidate is entitled to as many observers as necessary to observe the actual counting of the ballots. The observer may note the names of those voting so that the candidates may be able to ascertain whether unauthorized persons voted in the election. The observers should be placed so that they do not compromise, or give the appearance of compromising, the secrecy of the ballot. The observer is not required to be a member of the labor organization unless that union's constitution and bylaws require him to be a member. There is no prohibition on the use of alternate observers, when necessary, or on the candidate serving as his own observer. Observers do not have the right to count the ballots.

And, the Department's regulations at 29 CFR 452.107(c) state that in any secret ballot election which is conducted by mail, regardless of whether the ballots are returned by members to the labor organization office, to a mail box, or to an independent agency such as a firm of certified public accountants, candidates must be permitted to have an observer present at the preparation and mailing of the ballots, their receipt by the counting agency and at the opening and counting of the ballots.

Further, the Department's regulations at 29 CFR 452.110(a) state, in part, that the Act contains a general mandate in Section 401(c), that adequate safeguards to insure a fair election be provided. A labor organization's wide range of discretion regarding the conduct of elections is thus circumscribed by a general rule of fairness.

Preservation of records

Section 401(e) of the LMRDA provides that "[t]he election officials designated in the constitution and bylaws or the secretary, if no other official is designated, shall preserve for one year the ballots and all other records pertaining to the election." 29 U.S.C. 481(e).

The Department's regulations at 29 CFR 452.106 state that in every secret ballot election which is subject to the Act, the ballots and all other records pertaining to the election must be preserved for one year. The responsibility for preserving the records is that of the election officials designated in the constitution and bylaws of the labor organization or, if none is so designated, its secretary. Since the Act specifies that ballots must be retained, all ballots, marked or unmarked, must be preserved. Independent certification as to the number and kind of ballots destroyed may not be substituted for preservation. In addition, ballots which have been voided, for example, because they were received late or because they were cast for an ineligible candidate, must also be preserved.

C. Court Cases

With passage of the LMRDA, Congress sought to "protect the rights of rank-and-file members to participate fully in the operation of their union through processes of democratic self-government." *Wirtz v. Hotel, Motel and Club Employees Union*, Local 6, 391 U.S. 492 (1969). The Supreme Court and other courts have recognized that with respect to union officer elections

covered by the LMRDA, "Congress' model of democratic elections was political elections in this country." *Id.* at 502.

This parallel between political elections and union officer elections extends to the interpretation of the LMRDA's ballot secrecy provisions. *See Marshall v. Local Union 12447, United Steelworkers of America, AFL-CIO,* 591 F.2d 199, 205 (3d Cir. 1978) ("… the facilities available for balloting [in union elections] are… similar to their use in political elections in this country, *i.e.*, in such a manner that voters cannot be identified with their choices."). Several cases make clear that the requirement of a secret ballot in union officer elections is to be interpreted strictly: if there is any possibility that a voter can be connected with his or her vote, the procedure does not comply with the LMRDA. *Id.* at 203 ("The definition [of secret ballot] is phrased in mandatory terms: the ballots must be marked in such a manner that the voter cannot be identified with his choice."); *Brennan v. Local 3489, United Steelworkers of America, AFL-CIO*, 520 F.2d 516, 522 (7th Cir. 1975) ("The statutory mandate is for a vote that "cannot" be identified with the voter.").

Courts have further clarified that the secret ballot requirement not only applies to the act of voting itself, but "any post-voting procedure designed to determine how individual union members voted or would have voted." *Reich v. District Lodge 720, International Association of Machinists and Aerospace Worker,* 11 F.3d 1496, 1500 (9th Cir. 1993); *see also Bachowski v. Brennan,* 413 F.Supp 147, 150 (W.D. Pa. 1976). Finally, although "electronic voting systems" are often designed and administered by third parties, the ultimate responsibility for upholding the

ballot secrecy requirement remains with the union. *See Local 3489*, 520 F.2d at 522; *Local Union 12447*, 591 F.2d at 204 (3d Cir. 1978).

As of the publication of this RFI, there are no published cases that apply these well-established principles of ballot secrecy to electronic voting systems. The Department addressed the issue in one court proceeding against the Allied Pilots Association in 2007, but the litigation was resolved without a judicial determination. In that union officer election, the union utilized an Internet and telephone voting system designed by a third-party company. To log into the electronic voting system to cast a vote, each member was required to enter an employee identification number (EIN), which was published on the union website, along with a randomly-generated personal identification number (PIN) assigned privately. This information was transmitted to a "member database" on a computer server maintained by the third-party company. This "member database" contained members' names, their EINs, and their PINs. If the EIN and PIN entered by members matched those on the "member database," the system permitted the members to cast their votes, which were recorded in a separate "vote database." However, the electronic voting system also generated number identification markers that linked the members with the votes they cast, which could be accessed by certain employees of the third-party company. Additionally, several individuals from the organization administering the election had access to members' EINs and PINs, which gave them the ability to log onto the voting system to determine how a member had voted. Upon these facts, the court found that the voting system violated the LMRDA requirements for ballot secrecy, but declined for other reasons to resolve the case on the parties' motions for summary judgment. *Chao v. Allied Pilots Ass'n*, 2007 WL 518586 (N.D. Tex. Feb. 20, 2007) (depublished). As a condition of the parties'

later settlement agreement, the District Court issued a Consent Decree and Order vacating its February 20, 2007 order. *Secretary of Labor v. Allied Pilots Ass'n*, Case 4:05-CV-338-Y (N.D. Tex. Jun. 13, 2007).

D. Legislation

After the disputed U.S. Presidential election in 2000, many states and localities mandated the purchase and use of electronic voting systems. The Help America Vote Act (HAVA) was signed into law in 2002. Pub. L. 107-252, 116 Stat. 1666 (42 U.S.C. 15301-15545). It was drafted, in part, in reaction to the controversy surrounding the 2000 Presidential election. HAVA provided funds for qualifying states to replace punched card voting systems or lever voting systems with new systems, including electronic systems, in accordance with HAVA's voting system standards. 42 U.S.C. 15302(a)(2). HAVA standards require all electronic voting systems to be auditable and produce a permanent paper record with a manual audit capacity available. 42 U.S.C. 15481(a)(2)(B). This mandatory paper record is the official record for recounts. *Id*.

Since 2002, a number of bills have been introduced in Congress that would require a voter verified paper audit trail (VVPAT) or verified paper record (VPR) in U.S. political elections. A VVPAT or VPR is intended as an independent verification system for voting machines designed to allow voters to verify that their vote was cast correctly, to detect possible election fraud or malfunction, to serve as an independent check on the record produced and stored by the electronic system, and to provide a means to audit the stored electronic results and allow for an accurate recount. Voter verified paper legislation introduced since 2002 include the following:

the Voter Confidence and Increased Accessibility Act of 2005 (H.R. 550, 109th Cong.), 2007 (H.R. 811, 110th Cong.; S. 2295, 110th Cong.), and 2009 (H.R. 2894, 111th Cong.; S. 1431, 111th Cong.); the Voting Integrity and Verification Act of 2005 (H.R. 704, 109th Cong.; S. 330, 109th Cong.), 2007 (S. 1869, 110th Cong.), and 2009 (S. 48, 111th Cong.); the Count Every Vote Act of 2005 (H.R. 939, 110th Cong.; S. 450, 109th Cong.) and 2007 (H.R. 1381, 110th Cong.; S. 804, 110th Cong.); and the Ballot Integrity Act of 2007 (S. 1487, 110th Cong.). None of these bills were passed in Congress. Although this national standard for voting has not yet been established, as of the publishing of this RFI, 32 states require VVPATs. VerifiedVoting.org, Voter-Verified Paper Record Legislation, http://www.verifiedvoting.org/article.php?list=type&type=13 (last visited Sept. 20, 2010). OLMS is not presently aware of an Internet voting system that offers voter-verified paper records or a manual audit.

E. Recent Developments

Electronic voting at polling stations using computer terminals or similar touch-screen machines which store and tabulate votes, but which are not Internet-based, are widely used in U.S. political elections. These are not on-line forms of voting, meaning the systems are not connected to the Internet.

Internet voting has not been widely adopted for political elections in this country and, in one situation, a Federal agency chose not to utilize Internet voting due to security concerns. *See* David Jefferson *et al*, *A Security Analysis of the Secure Electronic Registration and Voting*

Experiment ("SERVE"), available at http://servesecurityreport.org/paper.pdf (report advising against Department of Defense use of Internet voting in 2004 political elections for military serving overseas due to security concerns).[1]

Internet voting has been tested overseas in public elections in Switzerland, the United Kingdom, and Estonia. Bryan Mercurio, *Democracy in Decline: Can Internet Voting Save the Electoral Process?*, 22 J. Marshall J. & Info. L. 409, 409-51 (2004). Internet voting has also been tested in the U.S. as a voting option in the 2000 Democratic primary in Arizona and the Republican straw poll in Alaska in 2000. *Id.* Proponents of remote Internet voting make several arguments in its favor. R. Michael Alvarez & Thad E. Hall, *Point, Click, and Vote: The Future of Internet Voting* (2004) Voting would be more convenient for Internet users, allowing them to vote at home, at work, or anywhere the Internet is available. *Id.* Internet voting would be logistically easier for some disabled voters and for military personnel overseas. *Id.* Internet voting might encourage greater voter participation, particularly among younger Americans typically well-versed in using the Internet. *Id.* Internet voting could also lower the cost of voting. *Id.* However, there are still

[1]In March 2007, the Federal Voting Assistance Program (FVAP) and the Department of Defense's Business Transformation Agency released a Request for Information to solicit from industry electronic solutions for three absentee voting tasks: voter registration, ballot request, and blank ballot delivery. *See Department of Defense: Expanding the Use of Electronic Voting Technology for UOCAVA Citizens As Required by Section 596 of the National Defense Authorization Act for Fiscal Year 2007,* May 2007. http://servesecurityreport.org/DoDMay2007.pdf. (The acronym UOCAVA stands for *Uniformed and Overseas Citizens Absentee Voting Act.) See also Elections: Action Plans Needed to Fully Address Challenges in Electronic Absentee Voting Initiatives for Military and Overseas Citizens*, Government Accountability Office, June 2007. GAO-07-774. http://www.gao.gov/new.items/d07774.pdf. The FVAP program introduced in 2009 is not Internet or online voting. It is the electronic transmission and online marking of the absentee ballot. The voter would still print out the ballot and send it in like any regular absentee ballot. http://www.fvap.gov/global/news/nr19-2009.html

concerns regarding on-line computer security, viruses and attacks, voter fraud, unequal computer and Internet access (the "digital divide"), and potential disintegration of civic life by moving away from a community-based electoral process where voting at the polls is an observable act of citizenship. *Id.*

In 2007, the National Mediation Board ("NMB") announced that it would primarily conduct representation elections offering participants both Internet voting and telephone electronic voting. 34 NMB No. 13, at 71 (Jan. 29, 2007) (Introduction of Internet Voting/Mock Election); 34 NMB No. 41, 200, 206 (Sept. 14, 2007) (Internet Voting Comment Period). The NMB adopted Internet voting based on its conclusion that "offering Internet voting in addition to phone voting will further its mission and enhance the Board's ability to conduct representation elections fairly and effectively." *Id.*

However, the Department's responsibility over union elections differs from NMB's in at least two ways. First, unlike the LMRDA which requires union officer elections to be conducted by secret ballot, the Railway Labor Act (RLA), which the NMB enforces, has no such ballot secrecy requirement. In a section titled, "Statutory Difference Between LMRDA and RLA," the NMB discussed LMRDA section 401(a)'s specific election standards, particularly its requirement of a secret ballot. It then drew a contrast with the RLA. "The language of the RLA gives the Board broad discretion in conducting representation elections. Section 2, Ninth provides that the Board "shall be authorized to take a secret ballot of the employees involved, *or to utilize any other appropriate method of ascertaining the names of their duly designated and authorized representatives*," and further that the Board may "establish the rules to govern the election." 34

NMB No. 41, 200, 206 (Sept. 14, 2007) (Emphasis in original.) Second, the NMB conducts representation elections itself and maintains direct control (along with its contractor) of the electronic voting system. In contrast, elections under the LMRDA are independently conducted by unions. The Department's involvement in an election is not triggered until a post-election complaint is filed, whereupon the Department investigates and, if the claim is substantiated, seeks a remedial election either through a voluntary settlement or by filing a complaint in district court. Because the Department does not have the degree of direct control over the electronic voting system that NMB has, and due to the heightened ballot secrecy requirements under the LMRDA, there are additional questions that must be addressed to ensure that the Department fulfills its legal obligations under the LMRDA.

II. Information Sought

The Secretary seeks public comment from interested parties to help the Department issue guidelines concerning the use of electronic voting systems in union officer elections. "Electronic voting systems" is meant to include: (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. The comments should help identify and describe what issues concerning the use of electronic voting systems in union officer elections should be addressed and what specific standards should be included in the guidelines. These guidelines and standards could further the Department's interest in ensuring compliance with LMRDA Title IV.

In particular, the Secretary is seeking written comments in response to the questions enumerated below. We request that all commenters identify themselves and any organizations or entities with which they are affiliated and generally describe their involvement or association with electronic voting systems. In responding to questions, please note and consider the preceding background information provided in Part I. Also, in your responding comments, please provide as much detail and specific examples as possible. Thank you for your cooperation and consideration.

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?

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?

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?

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

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?

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?

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?

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?

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?

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?

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?

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 afterwards?

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?

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?

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?

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?

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?

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?

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?

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?

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?

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?

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?

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.

Signed in Washington, DC, this 5th day of January, 2011,

//s// John Lund_____

John Lund,

Director, Office of Labor-Management Standards

Billing Code
4510-CP

<FRDOC> [FR Doc. 2011–311 Filed 1–10–11; 8:45 am]
<BILCOD>BILLING CODE 4510–86–P

[FR Doc. 2011-311 Filed 01/10/2011 at 8:45 am; Publication Date: 01/11/2011]