OLMS COMPLIANCE TIP

Electing Union Officers Using Remote Electronic Voting Systems

The Labor-Management Reporting and Disclosure Act (LMRDA) establishes democratic standards for conducting regular elections of union officers and elections of delegates who elect officers. The Office of Labor-Management Standards (OLMS), an agency within the Department of Labor, is responsible for enforcing the LMRDA. The LMRDA requires every local labor organization to elect its officers by secret ballot, and every national, international and intermediate labor organization to elect officers by secret ballot among the members in good standing or by representatives chosen by secret ballot. *See* 29 U.S.C. 481(a), (b), (d). The LMRDA further 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), and that the ballots and all other records pertaining to the election shall be preserved for one year following the election, 29 U.S.C. 481(e). The LMRDA also gives union members who believe that a violation of the election provisions of the LMRDA has occurred the right to file a complaint with the Secretary of Labor.

Purpose of this compliance tip:

This guidance has been developed by OLMS to explain how the LMRDA's requirements apply when implementing remote electronic voting systems in union officer elections. The challenges presented in assuring the secrecy and security of remote electronic voting systems have been well-documented in the context of public elections, which Congress used as the model for union elections under the LMRDA.[i] While remote electronic voting has not been widely adopted for public elections, technology to address these challenges has been a matter of extensive study and discussion. Two significant challenges are the tension between maintaining the secrecy of the ballot while ensuring that each eligible member's vote is accurately cast, and ensuring observability for a voting technology that does not necessarily generate "ballots" that can be observed at the "polls" and at their "counting," as the LMRDA provides. Because the technology in this field is evolving, it is difficult to identify definitive solutions that are most likely to permit voting that is in conformance with the LMRDA. Further, new technology is likely to provide additional methods of conducting remote electronic voting consistent with the LMRDA.[ii]

The specific guidance presented here is based on current technology and the characteristics and design elements of remote electronic voting systems that OLMS has reviewed to date. While all remote electronic voting systems must comply with the LMRDA's requirements, it is possible that solutions other than those identified here would also satisfy these requirements. Thus, OLMS will evaluate each electronic voting system that is the subject of a complaint under title IV of the LMRDA on a case-by-case basis to determine whether it meets the requirements of the statute. If you have questions about remote electronic voting systems, OLMS welcomes you to contact us at olms-public@dol.gov Moreover, OLMS recognizes that innovative voting technology may be developed that enhances compliance with the requirements of the LMRDA, and OLMS invites such innovative developments to be shared with us, also at olms-public@dol.gov

Remote electronic voting systems:

The LMRDA does not require a particular method or system of voting. Labor organizations may establish their own methods or systems of voting for officer elections as long as they are consistent with the LMRDA. Some labor organizations, in recent years, have chosen to conduct officer elections using remote electronic voting systems or have expressed interest in using a remote electronic voting system to elect their officers. The term "remote electronic voting systems" is meant to include: (1) electronic voting from remote site personal computers via the Internet; and (2) electronic voting from remote site telephones. It is not meant to include electronic voting machines used for casting votes at polling sites or electronic tabulation systems where votes are cast non-electronically but counted electronically (such as punch card voting or optical scanning systems). As with other voting procedures, remote electronic voting systems may be permissible under the statute so long as they satisfy the LMRDA's standards.

1. ***Guidance for preserving ballot 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). Several court cases make it clear that the requirement of a secret ballot in union officer elections is to be interpreted strictly. Ballot secrecy requires that no person, including an independent third party, have access to information allowing such person to learn how a particular member cast his or her vote at any time. Moreover, a member's vote must remain secret after the ballot is cast.

One way to help to insure that ballot secrecy is maintained in an electronic voting system is to avoid creating a connection between a voter's identity and the vote cast, *i.e.*, voters' names would never be entered into the system as part of the voting credentials (the term "credentials" in this guidance includes the multiple codes used for various purposes in electronic voting systems, including access codes, log-in codes, confirmation codes, etc.). In this way a voter's identity could never be linked to his or her vote using information in the system. This can be accomplished by determining voter eligibility prior to mailing the voting credentials and by randomly assigning the credentials to each eligible voter. Once this initial eligibility determination is made and the credentials mailed, there can be no mechanism to void or prevent the casting of ballots by any members who were determined to be eligible. Such a system, however, can present logistical challenges. For example, a union may need to provide replacement credentials to members who have not received or have lost their voting credentials or issue such credentials to newly eligible members. If duplicate credentials or other processes are used to resolve these logistical challenges, all material must be secured when not in use and observers must be given the opportunity to observe the processes employed when using the materials.

Systems should employ proper safeguards to prevent a voter from being able to provide visual proof of the content of his/her vote in order to prevent secrecy violations in the form of coercion or vote buying/selling. For example, the system must not display the voter credential and the content of the vote in such a way that it permits the voter to capture and share the image, nor should lists matching voter credentials and the content of the vote be publicly available.

To the extent that technology is developed for public elections that allows for the inclusion of voter-identifying information in a manner that protects vote secrecy, that technology may also be appropriate for use in union elections.

2. ***Guidance for preserving observer rights***:

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). This requirement provides for the essential monitoring that votes were cast by eligible union members and that those votes were accurately tallied. In the context of electronic voting systems, in which the "polls" and "tally" are not visible, assuring the integrity of such systems presents challenges.

The Department's regulations have permitted the conduct of election by mail ballot, as long as safeguards are followed to protect secrecy and to allow observation of specific stages of the election process, namely, the preparation and mailing of the ballots, their receipt by the counting agency, and the opening and counting of the ballots. 29 CFR 452.97, 107(c). Similar procedures in the context of electronic voting, which permit observation and protect the security of the vote from its casting to its counting, must include:

a) The opportunity to view the list of members and make eligibility challenges prior to the distribution of voter credentials.

b) The opportunity to observe the preparation and distribution of voting credentials to be used by members. Observers must be allowed to view the process, but must not be allowed to see the specific voting credentials that are sent to individual members, which must be kept secret.

c) The opportunity to observe any later distribution of credentials to members who did not receive or who lost credentials. Again, observers must be allowed to view the process, but must not be allowed to see what specific voting credentials are sent to individual members, which must be kept secret.

d) The use of technology that protects the integrity of the vote from the point when it is cast by the voter through the voting process, such as client-side encryption technology, that runs on the voter's computer or in conjunction with any computer-telephone integration, rather than on the election server.

e) The opportunity to observe any steps necessary for the counting of the votes, and any other steps necessary to audit that process.

f) The use of technology that provides a secure method of independent vote verification that allows the voter or an observer to confirm that the vote was recorded and counted accurately. Safeguards should be employed, however, to prevent such features from presenting secrecy lapses and opportunities for voter coercion. Safeguards that could preserve this aspect of observability without compromising vote secrecy may include:
   i. Allowing each member to view a printed ballot version of his or her electronic vote, which contains a credential known only to the voter and which is stored in a supervised, secure, observable location. These printed ballots could also be tallied in a supervised, secure, observable location to verify the accuracy of the electronic vote count.
   ii. Allowing each member to confirm the accuracy or integrity of his or her vote by inspecting a non-public list of the electronic votes alongside the credential known only to the voter, stored in a supervised, secure, observable location.
   iii. Allowing each member to confirm the accuracy or integrity of his or her vote by inspecting a posted list that pairs representations of votes (e.g., as hashes or codes that would allow a voter to know that the vote has not been changed but would not reveal the vote choice itself) alongside voter credentials, or representations of voter credentials.

The electronic voting system should contain mechanisms by which observers can verify, prior to an election, that the system is working properly.

The electronic voting system should include hash chains on the activity logs and the ballot box.

The electronic voting system should be audited by an authorized independent party periodically.

For any electronic voting system, there should be a document or documents that specify the security policy for all systems that will come into contact with the voter or vote information. Further, every role and its corresponding access should be clearly specified, using mathematical descriptions where applicable. The security policy should also include a risk assessment, threat analysis, and modifications made to mitigate such risks/threats.

3. Guidance for preserving records:

The electronic votes and any paper versions of the electronic votes, and all other paper and electronic records pertaining to the election, including eligibility lists, the voting credentials, the log files, the time stamped software code used to run the electronic voting system, and the ballot tally results, must be preserved for one year.

4. Guidance for preserving right to vote:

An alternative voting method must be provided, upon request, to any member who does not have access to the electronic voting system.

Remote voting must be implemented in a manner that does not create barriers for individuals with accessibility needs.

Office of Labor-Management Standards Field Offices

Atlanta, GA
Birmingham, AL
Boston, MA
Buffalo, NY
Chicago, IL
Cincinnati, OH
Cleveland, OH
Dallas, TX
Denver, CO
Detroit, MI
Ft. Lauderdale, FL
Honolulu, HI
Kansas City, MO
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
Nashville, TN
New Orleans, LA
New York, NY
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
St. Louis, MO
San Francisco, CA
Seattle, WA
Tampa, FL
Washington, DC

For the address and telephone number of our field offices, please call 1-866-4-USA-DOL (1-866-487-2365) , or view our online organizational listing at **http://www.dol.gov/olms/contacts/lmskeyp.htm**.

OLMS

Office of Labor-Management Standards
U.S. Department of Labor

October 2016

Visit us at **www.olms.dol.gov**
E-mail us at **olms-public@dol.gov**
Call the DOL National Call Center at **1.866.487.2365**

REFERENCES

[i] Nelson Hastings, et al.: Security Considerations for Remote Electronic UOCAVA Voting. National Institute of Standards and Technology, NISTIR 7770 (February 2011). *Available at*: http://www.nist.gov/itl/vote/upload/NISTIR-7770-feb2011-2.pdf.

[ii] U.S. Vote Foundation: The Future of Voting: End-to-End Verifiable Internet Voting Specification and Feasibility Assessment Study (July 2015). *Available at:* https://www.usvotefoundation.org/E2E-VIV.

ADDITIONAL RESOURCES

iVote Advisory Committee Final Report, Aug. 21, 2015, Utah Lt. Governor Spencer J. Cox

Peter Haynes, "Online voting, rewards and risks," Atlantic Council, (2014). *Available* at: http://www.atlanticcouncil.org/publications/reports/online-voting-rewards-and-risks

Barbara Simons and Douglas W. Jones, "Internet Voting in the U.S." (2012), 55 *Communications of the ACM* 68, http://cacm.acm.org/magazines/2012/10/155536-internet-voting-in-the-us/fulltext.

U.S. Election Assistance Commission (EAC), "A Survey of Internet Voting" (September 2011), http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf.

David Jefferson, "If I Can Shop and Bank Online, Why Can't I Vote Online?" https://www.verifiedvoting.org/resources/internet-voting/vote-online/

Association for Computing Machinery (ACM) U.S. Public Policy Council, "Issue Brief: Internet Voting and Uniformed and Overseas Citizens absentee Voters," http://usacm.acm.org/images/documents/IB_Internet_Voting_UOCAVA.pdf.

Drew Springal, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Maggie MacAlpine, J. Alex Haldermann, "Security Analysis of the Estonian Internet Voting System," *Proceedings of the 21st ACM Conference on Computer and Communications Security* (CCS '14) (November 2014), https://estoniaevoting.org/findings/paper/.