OLMS COMPLIANCE TIP

Electing Union Officers Using Remote Electronic Voting Systems[1]

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. While the LMRDA does not require a particular method or system of voting, and labor organizations may therefore establish their own methods or systems of voting for officer elections, those systems must be consistent with 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. 29 U.S.C. 482(a).

Purpose of this Compliance Tip:

This Compliance Tip[2] 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. See *Loc. 3489, United Steelworkers of Am., AFL-CIO v. Usery*, 429 U.S. 305, 309 (1977) ("The basic objective of Title IV of the LMRDA is to guarantee 'free and democratic' union elections modeled on 'political elections in this country[.]'"). In recent years, the use of internet voting systems to conduct public elections in the U.S. and in other countries has increased (as has its use in non-public elections), and the technology continues to evolve. Given the rapidly developing technology in this area, this Compliance Tip: 1) focuses on some of the factors that OLMS will consider, on a case-by-case basis, when evaluating any remote electronic voting system used in a union officer election; and 2) clarifies OLMS' position with regard to electronic voting.

[1] Throughout this Compliance Tip, we occasionally use the term "internet voting" as a shorthand phrase to describe the technologies used for remote electronic voting systems. Both the terms "internet voting" and "remote electronic voting systems" are meant to include: (1) electronic voting from remote site personal computers via the internet; and (2) electronic voting from remote site telephones. They are 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).

[2] This Compliance Tip updates a prior version that was first published in October 2016.

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. 29 U.S.C. 481(c).

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.

In the sections below, based on our understanding of the technology currently available, we set out guidance regarding procedures for reserving ballot secrecy, observer rights, the right to vote, and election records. Ballot secrecy and observer rights are specific requirements contained in the LMRDA and operate together with the more general obligations to preserve the right to vote and to provide "[a]dequate safeguards to insure a fair election," subjects this guidance also addresses. We also include guidance on the LMRDA's record preservation requirements and guidance regarding preservation of the right to vote as they relate to internet voting.

Before setting out guidance on these subjects, there are four foundational observations that inform OLMS' approach to complaints regarding internet elections:

- First, this Compliance Tip does not purport to lay out the only ways by which an internet voting system can meet Title IV's requirements. Nor does this Compliance Tip offer unions safe harbor if events occur that call into question whether an election met the requirements of the LMRDA. The investigations of complaints made under Title IV are fact-based, and OLMS is required to investigate all the facts surrounding any complaint alleging a violation of Title IV and base its decision on the investigative findings.
- Second, the LMRDA's statutory standards for ballot secrecy, 29 USC 402(k), are not changed by this Compliance Tip and OLMS will continue to apply existing standards to all voting systems, including remote electronic voting systems. Some of these systems present secrecy issues because, by their operation, they create a persistent electronic link between a voter and their vote. However, there are system protections that may exist to prevent access to this link, some of which are discussed below. With those protections in mind (and others that service providers may develop), OLMS will continue to assess the totality of the facts uncovered (including whether such protections were actually used) in any investigation of a complaint alleging that the secret ballot provisions of the Act were violated in a way that may have affected the outcome of an election. However, OLMS will not conclude that the existence of a persistent electronic link between a voter and their vote is, in and of itself, a violation of the Act.
- Third, the LMRDA's statutory standards for observer rights, 29 USC 481(c), are not changed by this Compliance Tip. However, OLMS recognizes that it may be impossible for a candidate's observer to observe an internet voting system in operation in the same way an observer can observe certain components of a polling site or mail ballot election. OLMS recognizes that there may be different methods for meeting the LMRDA's observer requirements, including indirect observation (*e.g.,* by way of an observer's inspection of open-source code at the observer's cost or through a certified audit by a reputable third party). OLMS does not endorse any particular auditor, nor has it sought to validate the code of any particular system.

As is the case with complaints alleging violation of the Act's secret ballot provisions, OLMS will assess the totality of the facts uncovered in any investigation of a complaint alleging that the observer provisions of the Act were violated in a way that may have affected the outcome of an election. However, OLMS will not find a violation of the Act's observer protections if, after an investigation, the facts establish that members had an opportunity to observe those parts of the election process that are observable through traditional methods and to confirm that a voting system accurately recorded votes as cast and accurately counted the recorded votes through 1) a member's inspection of open source code at their own cost; 2) reliance on a system auditor; or 3) some other meaningful opportunity to observe the electronic balloting process.

- Finally, with respect to the LMRDA's requirement that "adequate safeguards to insure a fair election shall be provided" as it applies to internet elections, 29 U.S.C. 481(c), this Compliance Tip contains suggestions that may mitigate the threats posed by malicious outside actors or malware and the chilling effects that these threats may pose as well as risks that any persistent electronic links between a voter and their vote has resulted in an actual breach of secrecy. Implementation of the suggestions contained in this Tip may also provide greater confidence to a union's members in the integrity of the system generally.[3] While the LMRDA does not require the integration of the security features discussed below into an internet voting system, nor is their use a guarantee that an election will be immune from challenge, OLMS will consider implementation of these protections, and others that providers may develop, during any investigation of a complaint alleging that adequate safeguards were not provided. As with all investigations, OLMS will assess the totality of the facts uncovered.

If you have questions about remote electronic voting systems, OLMS welcomes you to contact us at OLMS-Public@dol.gov.

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). Both ballot secrecy and the obligation to provide adequate safeguards to insure a fair election require that appropriate procedures be in place and enforced throughout the process to protect union members from having their voting selections exposed, both while they are casting their ballots and after their ballot is cast. Communicating these procedures to members prior to the election helps members understand the security surrounding their ballot choices.

[3] The literature on voting integrity refers to some of these safeguards as End-To-End Verification (see, e.g. "End-to-End (E2E) Verifiable Protocols for Voting Systems" (Benaloh, Rivest, Ryan, Stark, Teague & Vora)), Risk Limiting Audits (see, *e.g.* "A Gentle Guide to Risk-Limiting Audits" gentle12.pdf (berkeley.edu) (Lindeman and Starks)), Logic and Accuracy Testing (see, e.g. "Logic and accuracy testing: A fifty-state review" (Logic and Accuracy Testing - A Fifty-State Review.pdf) (Walker, Bajaj, Crimmins & Halderman) and "Improving the Security of United States Elections with Robust Optimization (arxiv.org)" (Crimmins, Halderman, and Sturt). OLMS' inclusion of these procedures and the references discussing them is for guidance only and should not be understood to create either (i) a set of requirements or a safe haven in the event a member files a complaint alleging that an election did not meet the secret ballot, observer or adequate safeguards provisions of Title IV, or (ii) an endorsement of any particular methodology or technology provider described therein.

Some remote electronic voting systems present secrecy issues because, by their operation, they create a persistent electronic link between a voter and their vote.[4] When investigating a complaint alleging that the secret ballot provisions of the Act were violated in a way that may have affected the outcome of the election, OLMS will not conclude the mere existence of a persistent electronic link between a voter and their vote is, in and of itself, a violation of the Act. Rather, OLMS will apply the standards of 29 U.S.C. 402(k) and will assess the totality of the facts uncovered through an investigation. Specifically, OLMS will consider whether a remote electronic voting system adequately employed protections, such as those listed below, to preserve voter secrecy in compliance with LMRDA standards by inhibiting unauthorized access to any persistent electronic link. While this list is not exhaustive, nor is every safeguard required, factors that OLMS would view favorably in terms of preserving ballot secrecy include:

- Allowing union members to vote only through a secure portal, such as those that include multi-factor authentication.
- Randomizing the order in which votes are stored in the encrypted file so that the ballot tally reveals no information about the order in which votes were cast.
- Ensuring that any voting credentials provided to members are not available to others, through union or company websites or in some other manner.
- Storing the returned electronic ballots in an encrypted file(s) that may be accessed only through the simultaneous use of multiple decryption keys distributed to a diverse group of actors (*e.g.*, representatives of competing candidates and one or more neutrals such as representatives of the election services provider or some other independent neutral entity that engages in election supervision) and only to produce an official tally of ballots.
- Employing safeguards that can detect and log efforts to breach the encrypted file and access information about how particular voters voted.
- Using technology that can prevent ballot image capture and sharing.[5]

2. Guidance for providing adequate safeguards to ensure a fair election, including 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.

[4] Not all remote electronic voting systems create these persistent links. To avoid creating these connections, voters' identifying information 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, randomly assigning the credentials to each eligible voter, and never creating a trail between the credential and the voted ballot.

[5] Some electronic voting systems include features that allow a voter to create visual proof of the contents of their ballot as cast. Such ballot image capture capacity is not unique to internet voting and is not, without more, a violation of the secret ballot provisions of the LMRDA. The potential consequences of ballot image capture (*e.g.,* vote buying or selling and voter coercion) may, however, violate the Act. OLMS will investigate allegations of such conduct and will determine whether the conduct violated the Act and, if so, whether the conduct may have affected the outcome of the challenged election. Nevertheless, systems that prevent image capture remain one type of safeguard labor organizations may consider employing to protect against violations of the Act.

The Department's regulations have permitted the conduct of election by mail ballot, as long as safeguards are followed 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 C.F.R. 452.107(c).

Some parts of an internet election process are observable in the traditional way; the opportunity to view the list of members and make eligibility challenges prior to the distribution of voter credentials and the loading of the ballots and voting credentials into the system, for example. Beyond this direct observation, there may be methods that provide additional opportunities to observe remote electronic voting systems. While this list is not exhaustive, nor is every procedure required, factors that OLMS would view favorably include:

- Using encryption technology meeting industry standards that ensures the integrity of the ballots at all points from when they are cast to decryption and counting and disclosing the use of such encryption technology to observers.
- Giving observers the opportunity to inspect the system's source code directly through the use of open-source code, or indirectly through a certified audit by a reputable third party.
- Mechanisms by which observers can verify, prior to an election, that the system is working properly, such as permitting observers to watch a test run on practice ballots to verify that the system records and tallies votes accurately.
- System-generated alerts made contemporaneously to observers if someone attempts to electronically tamper with the election while in progress.
- The opportunity to observe the preparation and distribution of voting credentials to be used by members (including subsequent distributions to members who did not receive or who lost credentials). 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.
- The opportunity to observe any steps necessary for the counting of the votes, and any other steps necessary to audit that process.
- Maintenance of detailed logs of every transaction and means to ensure the integrity of those logs.
- Periodic audits of the system by an authorized independent party.

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. Documentation helps establish that the procedures are followed consistently, provides a reference for future use, and helps to ensure that the procedures are updated as the system or technology changes. Documentation of electronic security procedures also enables auditors and regulatory bodies to ensure that the system is in compliance with applicable laws and regulations.

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, encrypted ballot files (protected in the same manner as during the election), and the ballot tally results, must be preserved for one year. For systems in which there is a persistent electronic link, it may be desirable for a union to destroy the encrypted ballot files after the later of the passage of one year or the conclusion of any post-election Title IV investigation or litigation or other records retention laws.

4. Guidance for preserving right to vote:

Either a union-provided access to an internet voting site or some other voting method must be provided, upon request, to any member who does not have access to the internet. Internet voting must be implemented in a manner that does not create barriers for individuals with accessibility needs.

If you have any questions, please email us at OLMS-Public@dol.gov or contact your nearest OLMS field office.

OLMS

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

Issued October 2016; Technical Revision September 2019;
Updated December 10, 2024 (footnote 4 corrected on December 12, 2024)

Visit us at www.dol.gov/olms
E-mail us at olms-public@dol.gov
Call us at (202) 693-0123