NATIONAL RIGHT TO WORK LEGAL DEFENSE FOUNDATION, INC.
8001 BRADDOCK ROAD, SUITE 600, SPRINGFIELD, VIRGINIA 22160 • (703) 321-8510

RAYMOND J. LAJEUNESSE, JR.
Vice President & Legal Director

FAX (703) 321-8239
***Home Page* http://www.nrtw.org**
***E-mail* rjl@nrtw.org**

June 23, 2010

By FAX & First Class Mail

Chairman Wilma B. Liebman
Members Peter C. Schaumber, Craig Becker, and Mark G. Pearce
National Labor Relations Board
1099 14th Street, N.W.
Washington, DC 20570

Re: Solicitation No. RFI-NLRB-01 (June 9, 2010)

Dear Chairman Liebman and Members Schaumber, Becker, and Pearce:

On June 9, 2010, the Board's contracting office issued a request through the federal government procurement process for information on "industry solutions regarding the capacity, availability, methodology, and interest of industry sources for procuring and implementing secure electronic voting services for both remote and on-site elections." (RFI-NLRB-1.) That request subsequently came to our attention through news reports.

Although the National Right to Work Legal Defense Foundation is not in the "industry" of providing electronic voting services, the Board's method of conducting representation and decertification elections is of great interest to the Foundation, because Foundation attorneys regularly advise workers opposed to unionization about their legal rights before, during and after such elections and, when necessary, represent such workers in legal proceedings related to those elections, *e.g.*, *Dana Corp*., 351 N.L.R.B. 434 (2007), and *Saint-Gobain Abrasives, Inc.*, 342 N.L.R.B. 434 (2004). The Foundation, therefore, has a unique perspective and significant practical experience to aid the Board in determining whether electronic voting services can accurately, fairly, safely and securely be used to carry out the Board's statutory mandate to conduct representation and decertification elections by "secret ballot," 29 U.S.C. § 159(c), (e).

The Board wants to know whether "mail, telephone, [or] web-based . . . voting . . . includes the necessary safeguards to ensure the accuracy, secrecy, observability, transparency, integrity, accountability, and auditability of Agency-conducted elections." (RFI-NLRB-01.) The short answer is that, unless Board agents are going to be present at all times at all remote voting sites, no *remote* mail or electronic voting system can be "free from distractions or other interferences, including undue intimidation or coercion," (*id.).*

Foundation attorneys regularly receive reports from workers of coercion, intimidation, and/or misrepresentation by union organizers, and peer pressure by fellow employees who are union militants, in the gathering of union authorization cards or signatures on union petitions for representation elections. Nothing could prevent the same kinds of coercion, intimidation, misrepresentation, and peer pressure in remote voting. Union organizers would be free to visit workers at their homes, conduct parties for workers at which alcoholic beverages and pressure are applied to obtain votes, and "invite" workers anywhere they are found to cast votes for the union on the organizers' Blackberries, notebooks, laptops, or cell phones or to mark ballots "yes" for the union that the organizers will "kindly" mail for them.

All forms of remote electronic or mail voting have the same defects as the card-check process that Congress has declined to adopt by rejecting the misleadingly named "Employee Free Choice Act" (EFCA), defects which the Board itself recognized in *Dana Corp*.: "unlike votes cast in privacy by secret Board election ballots, [remote votes could be] public actions, susceptible to group pressure exerted at the moment of choice"; (2) "union [remote voting] solicitation campaigns [could be] accompanied by misinformation or a lack of information about employees' representational options"; (3) "a Board election presents a clear picture of employee voter preference at a single moment," while remote voting would "take place over a protracted period of time" during which "employees can and do change their minds about union representation"; and, (4) "the Board will invalidate elections affected by improper electioneering tactics, and an employee's expression of choice is exercised by casting a ballot in private," but there "are no guarantees of comparable safeguards in [a remote voting] process," during which Board agents would not be present to see that coercion, intimidation, or misrepresentation has occurred and ballots would not necessarily be cast in private. 351 N.L.R.B. at 438–39.

By permitting mail balloting only "where circumstances tend to make it difficult for eligible employees to vote in a manual election or where a manual election, though possible, is impractical or not easily done," the Board's *Casehandling Manual*, § 11301.2, implicitly acknowledges that mail balloting is less reliable than secret balloting at polling places monitored by Board agents and the parties' observers. In 1994, the Board considered amending its *Casehandling Manual* to use mail ballots in a broader range of situations. However, Regional officers filed comments against the expansion, at least one of which pointed out the risk of coercion or intimidation that exists with mail ballots: "The presence of a Board agent at an election gives employees a greater sense of security . . . . [T]he potential for interference by any party in a mail ballot situation [outweighs] . . . any cost savings which might result." *Daily Lab. Rep. (BNA)* No. 145, at AA2-3 (Aug. 1, 1994).

Academic studies confirm our intuitive and experience-based conclusion that remote electronic voting, like mail balloting, will not provide the "secret ballot" elections Section 9 of the Act mandates. The Report of the National Workshop on Internet Voting, sponsored by the National

Science Foundation and published by the Internet Policy Institute in March 2001, concluded that remote internet voting

> poses substantial security risks . . . . Without official control of the voting platform and physical environment, there are many possible ways for people to intervene to affect the voting process and the election results. Current and near-term technologies are inadequate to address these risks.

With regard to "Secrecy and Non-Coercibility" in particular, that report said (emphasis added):

> In a controlled environment, such as the poll site, election officials and observers can ensure that people cast their ballots unimpeded by any outside influence. Conversely, *remote voting—over the Internet or by conventional [mailed paper] absentee ballots—can be observed [by outsiders], opening the door to the possibilities of vote selling and coercion*. . . .
>
> Remote Internet voting also poses additional threats to the integrity of elections beyond those of paper absentee ballots. First, for those who access the Internet from [a] workplace, systems administrators can often monitor or record the activity at each workstation. This presents an opportunity for monitoring and coercion that is unlikely to occur with paper absentee ballots. Second, the distributed nature of the Internet could facilitate schemes for large-scale, automated vote selling or trading that would be more difficult with paper ballots.
>
> . . . . *Absent a controlled environment, there is no way to guarantee that some degree of coercion will not occur*, especially within families, or in institutional settings . . . .

A more recent report on the feasibility of remote internet, postal voting, and postal voting with automated counting agreed that all of these methods of voting make coercion possible:

> Respecting confidentiality means that voters vote alone and without any coercion. *None of the remote voting modes in an uncontrolled environment that we examine is able to guarantee that the elector expresses his choice alone and free from coercion*.

Chantal Enguehard & Rémi Lehn, *Vulnerability analysis of three remote voting methods*, XXI IPSA World Congress of Political Science (July 13, 2009), at 9 (emphasis added). This study also concluded that "[n]one of the remote voting systems can be classified as safe." *Id*. at 12. However, it emphasized that internet voting is even less secure than postal voting:

> Internet voting presents vulnerabilities of the worst kind: they are invisible, can affect a large number of votes, may be committed by a small number of people (from anywhere in the world) and do not require expensive equipment. These vulnerabilities are present at different stages of the voting process: at the voter's computer, during the delivery of votes or when the count is processed.

Id. These vulnerabilities include fraud, both at the point of transmission and in reception and counting. *See id*. 6-7, 11.

In sum, unless all voting in representation and decertification elections is done by workers in privacy at sites monitored by Board agents and observers from both union and employer, remote voting is a bad idea whose time should never come, because it will facilitate coercion, intimidation, and fraud. The Board should not use this proposal to grant labor organizations what they have been unable to gain from Congress through passage of EFCA: destruction of the secret ballot.

Respectfully submitted,

Raymond J. LaJeunesse, Jr.

cc: Douglas S. Wolf, Contracting Officer (via e-mail to doug.wolf@nlrb.gov)

RJL/rpc