epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

September 28, 2016

The Honorable William Hurd, Chairman
The Honorable Robin Kelly, Ranking Member
Subcommittee on Information Technology
U.S. House Committee on Oversight & Government Reform
2157 Rayburn House Office Building
Washington, DC 20515

RE: Hearing on "Cybersecurity: Ensuring the Integrity of the Ballot Box"

Dear Chairman Hurd and Ranking Member Kelly:

The Electronic Privacy Information Center ("EPIC") is a public interest research center established more than 20 years ago to focus public attention on emerging privacy and civil liberties issues. EPIC has a long history of working to protect voter privacy and election integrity.[1] EPIC, Verified Voting, and Common Cause last month released *The Secret Ballot at Risk: Recommendations for Protecting Democracy*, a report highlighting the right to a secret ballot and how Internet voting threatens voter privacy.[2] We have submitted a copy of the report with this letter. Additionally, in April 2015, as the result of a Freedom of Information Act lawsuit,[3] EPIC obtained a September 2011 report about online voting from the Department of Defense. The report, produced in response to EPIC's July 2014 FOIA request,[4] summarizes a pilot test of e-voting system. The report recommends several changes, including accessibility and user interface, but does little to address privacy and security concerns except for recommending "visible security features" to "give users greater confidence in the privacy and security of their ballots." EPIC has also previously submitted comments and testified before the Election Assistance Commission.[5]

[1] Voting Privacy, EPIC, https://epic.org/privacy/voting/.
[2] Caitriona Fitzgerald et al., *The Secret Ballot at Risk: Recommendations for Protecting Democracy* (2016), http://secretballotatrisk.org.
[3] EPIC v. Dep't of Defense, EPIC, https://epic.org/foia/dod/e-voting/.
[4] EPIC, FOIA Request to Dep't of Defense (July 17, 2014), https://epic.org/privacy/voting/EPIC-FVAP-FOIA-Request-071714.pdf.
[5] *See* EPIC Comments to Election Assistance Comm'n (May 5, 2008), *available at* https://epic.org/privacy/voting/2007vvsg_5508.pdf; *see also* EPIC Comments to Election Assistance Comm'n (April 24, 2008), *available at* https://epic.org/privacy/voting/eac_test4_24.pdf.

The Secret Ballot

The right to cast a secret ballot in a public election is a core value in the United States' system of self-governance. Secrecy and privacy in elections guard against coercion and are essential to integrity in the electoral process. Secrecy of the ballot is guaranteed in state constitutions and statutes nationwide. However, as states permit the marking and transmitting of marked ballots over the Internet, the right to a secret ballot is eroded and the integrity of our elections is put at risk.

Since its widespread adoption in 1896, the concept of the secret ballot has remained a cornerstone of our democratic process. In the 1992 case of *Burson v. Freeman*, the Supreme Court described voter privacy as a means of preventing voter fraud while protecting against undue coercion.[6] Upholding a Tennessee statute that prohibited political candidates from campaigning within 100 feet of a polling place entrance, the Court stated:

> [A]n examination of the history of election regulation in this country reveals a persistent battle against two evils: voter intimidation and election fraud. After an unsuccessful experiment with an unofficial ballot system, all 50 States, together with numerous other Western democracies, settled on the same solution: a secret ballot secured in part by a restricted zone around the voting compartments. We find that this widespread and timetested consensus demonstrates that some restricted zone is necessary in order to serve the States' compelling interests in preventing voter intimidation and election fraud.[7]

Because of the documented history of voter intimidation, coercion, and fraud associated with third party knowledge of how individual voters cast their ballots, it is important not to underestimate the importance of voter privacy. No community is immune to the effects of voter manipulation, but some communities are more vulnerable than others—for example minorities, new citizens, or the poor. Our need for privacy protections is just as strong today as it was when the secret ballot was adopted.

Federal and state courts and legislatures have historically taken measures to protect the right of voters to vote their conscience without fear of retaliation.[8] Our findings in *The Secret Ballot at Risk: Recommendations for Protecting Democracy* showed that 44 states have a constitutional provision guaranteeing that secrecy in voting shall be preserved.[9] Some states, such as Alabama, provide an individual right to a secret ballot.[10] Others, such as Delaware, require the state legislature to prescribe laws protecting ballot secrecy.[11] The six states (and DC)

---

[6] *Burson v. Freeman*, 504 U.S. 191 (1992).

[7] *Id.* at 206.

[8] *See id.*

[9] AK, AL, AR, AZ, CA, CO, CT, DE, FL, GA, HI, IA, ID, IL, IN, KS, KY, LA, MA, MD, ME, MI, MN, MO, MS, MT, NC, ND, NE, NM, NV, NY, OH, PA, SC, SD, TN, TX, UT, VA, WA, WI, WV, WY.

[10] *See e.g.* Ala. Const. Art. VIII, § 177, as amended by Ala. Const. Amend. No. 865.

[11] *See e.g.* Del. Const. art. 5 § 1.

that do not have a constitutional provision regarding ballot secrecy have statutory provisions referencing secrecy in voting.[12]

Despite the strong recognition of the importance of the secret ballot in state constitutions and statutes, state governments are experimenting with Internet voting in public elections. Our state survey found that 32 states and D.C. offer Internet voting to at least some voters, typically military and overseas voters.[13] In Alaska, all absentee voters can vote via the Internet. In Utah, voters with disabilities are also allowed to use the system. Of the 32 states and D.C. that offer some form of Internet voting, voters in 28 of those states and D.C. are explicitly required by state elections officials to sign a waiver of their right to a secret ballot in order to vote over the Internet. In the five other states, voters are permitted to cast ballots via the Internet with no warning from elections officials that their ballot may not remain secret.[14]

Internet voting will erode voter privacy and threaten election integrity. We need look no further than the warning all Alaska voters receive if they use the online voting system to cast their absentee ballots. Alaska acknowledges that the system is insecure and may not work, warning voters that "[w]hen returning the ballot through the secure online delivery system, your [sic] are voluntarily waving [sic] your right to a secret ballot and are assuming the risk that a faulty transmission may occur."[15] A similar warning on a physical polling place voting system would be considered unacceptable.

Recommendations on Voting and Privacy

1. Ballot secrecy and voter privacy should be the terms used to describe privacy within the context of voting technology standards as well guidelines related to certification and testing.
2. Ballot secrecy and voter privacy must be core values within the context of voting technology standards and testing and certification of voting systems.
3. Full sections on voter privacy should be included in each of the standards sections that address system operation.
4. Implement fail‐safe approaches to ensure that when voting systems fail or malfunction they do so in a way that protects ballot secrecy, accuracy of the votes recorded, retained, and reported in final election results.
5. Internet voting should not be implemented in any public election.

[12] DC, NH, NJ, OK, OR, RI, VT.
[13] AK, AL, AZ, CA, CO, DC, DE, FL, HI, IA, ID, IN, KS, LA, MA, ME, MO, MS, MT, NC, ND, NE, NJ, NM, NV, OK, OR, RI, SC, TX, UT, WA, and WV all offer some form of Internet voting.
[14] Caitriona Fitzgerald et al., *The Secret Ballot at Risk: Recommendations for Protecting Democracy* 7-8 (2016), http://secretballotatrisk.org.
[15] State of Alaska Division of Elections, *Absentee Voting by Electronic Transmission*, http://www.elections.alaska.gov/vi_bb_by_fax.php.

We look forward to working with you to ensure that voter privacy is protected in this election and elections to come.

Sincerely,

Marc Rotenberg
Marc Rotenberg
EPIC President

Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC State Policy Coordinator