epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

January 8, 2020

The Honorable Zoe Lofgren, Chairperson
The Honorable Rodney Davis, Ranking Member
Committee on House Administration
1309 Longworth House Office Building
Washington, D.C. 20515

Dear Chairperson Lofgren and Ranking Member Davis:

We write to you regarding the hearing on "2020 Election Security-Perspectives from Voting System Vendors and Experts."[1] EPIC believes the Committee should ensure that (1) voting systems accurately record votes and (2) the secret ballot is protected. These are two critical requirements for election security.

EPIC is a nonpartisan research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC has a long history of working to protect voter privacy and election integrity. We seek to ensure the integrity of voting equipment[3] and to preserve the secret ballot, the well-established right of individuals to remain anonymous while voting.[4] EPIC's advisory board includes distinguished experts in law, technology, and public policy, including several who have pioneered techniques for election security and privacy protection.[5]

---

[1] *2020 Election Security-Perspectives from Voting System Vendors and Experts*, 116th Cong. (2020), Comm. on H. Admin. (Jan. 9, 2020), https://cha.house.gov/committee-activity/hearings/2020-election-security-perspectives-voting-system-vendors-and-experts.

[2] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.

[3] *See* EPIC, Voting Privacy, https://epic.org/privacy/voting/; EPIC Comments Regarding the Proposed Voluntary Voting System Guidelines 20.0 Principles and Guidelines (May 29, 2019), https://epic.org/apa/comments/EPIC-USTPC-Comments-EAC-VVSG-May2019.pdf; Brief of Amici Curie EPIC, *Curling v. Raffensperger,* (N.D. Ga. Aug 15, 2019), https://epic.org/amicus/voting/curling/; EPIC Comments Regarding the 2009 Voluntary Voting System Guidelines Version 1.1, Election Assistance Comm'n (Sept. 28, 2009), https://epic.org/privacy/voting/epic_eac_comments_10-09.pdf..

[4] *See* Caitriona Fitzgerald, et al., *The Secret Ballot at Risk: Recommendations for Protecting Democracy* (2016), http://secretballotatrisk.org.

[5] *See, e.g.*, David Chaum, *Achieving Electronic Privacy*, Scientific American 96-101 (Aug. 1992); Stefan Brands, *Non-Intrusive Cross-Domain Digital Identity Management*, Presented at Proceedings of the 3rd Annual PKI R&D Workshop (Apr. 2004), *available at* http://www.idtrail.org/files/cross_domain_identity.pdf; Peter G. Neumann, National Computer Security Conference, *Security Criteria for Electronic Voting* (Sept. 20-23, 1993); Ronald L. Rivest & John P. Wack, *On the Notion of Software Independence in Voting Systems*, 366 Philosophical Transactions: Mathematical, Physical and Eng'g Sciences (Oct. 28, 2008); David L. Dill, Bruce Schneier & Barbara Simons, *Voting and Technology: Who Gets to Count Your Vote?*, 46 Communications of the ACM 29 (Aug. 2003); Whitfield

Electronic voting machines are subject to manipulation, attack, and fraud. In an extensive report concerning the integrity of voting systems and the risks associated with digital technology, the National Academies of Sciences recently determined:

> [A]ll digital information—such as ballot definitions, voter choice records, vote tallies, or voter registration lists— is subject to malicious alteration; there is no technical mechanism currently available that can ensure that a computer application— such as one used to record or count votes— will produce accurate results; testing alone cannot ensure that systems have not been compromised; and any computer system used for elections— such as a voting machine or e-pollbook— can be rendered inoperable.[6]

But this is not news. For many years, computer scientists and cybersecurity experts have warned election officials that paperless balloting systems are unreliable, insecure, and unverifiable.[7] The necessary criteria for electronic voting security have long been known[8] – but the voting system vendors repeatedly fail to meet them.[9]

The drive for perfecting the election process and voting technology is grounded in a fundamental promise of our form of democracy—one vote for each person. The bar for voting technology and election administration should be set high. Voters need voting systems and procedures that reflect the best that human factors, computer science, cryptography, data protection, security, computer architecture, and informatics can produce.

We ask that this statement be entered in the hearing record. EPIC looks forward to working with the Committee on these issues of vital importance to the American public.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

---

Diffie, *The Evolving Meaning of Information Security*, ACM Turing award lectures (2016), https://dl.acm.org/doi/pdf/10.1145/1283920.2949031.

[6] National Academies of Sciences, Engineering, and Medicine, et al. *Securing the Vote: Protecting American Democracy* 42, 80 (National Academies Press, 2018).

[7] *See* Eric A. Fischer, Cong. Research Serv., RL32139, *Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues* (2003) ("there appears to be an emerging consensus that in general, current DREs do not adhere sufficiently to currently accepted security principles for computer systems").

[8] Peter G. Neumann, National Computer Security Conference, *Security Criteria for Electronic Voting* (Sept. 20-23, 1993) (establishing the importance of reliability, accountability, and disclosability); U.S. Election Assistance Comm'n, Proposed Voluntary Voting System Guidelines 2.0 Principles and Guidelines, 84 FR 6775 (Feb. 28, 2019) (setting ballot secrecy, voter privacy, and auditability as fundamental principles), https://www.eac.gov/assets/1/6/TGDC_Recommended_VVSG2.0_P_Gs.pdf.

[9] J. Alex Halderman, Op-Ed., *I Hacked an Election. So Can the Russians*, N.Y. Times (Apr. 5, 2018).