epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

AND

U.S. TECHNOLOGY POLICY COMMITTEE OF THE ASSOCIATION FOR COMPUTING MACHINERY

to the

ELECTION ASSISTANCE COMMISSION

Notice of proposed Voluntary Voting System Guidelines 2.0 Principles and Guidelines request for public comment.

May 29, 2019

By notice published February 28, 2019, the Election Assistance Commission ("EAC") requested public comment on the proposed Voluntary Voting System Guidelines 2.0 Principles and Guidelines ("VVSG 2.0").[1]

EPIC and the U.S. Technology Policy Committee of the Association for Computing Machinery ("USTPC") support the proposed VVSG 2.0 and submit these comments to the EAC: (1) to commend the inclusion of strong principles protecting voter privacy, ballot secrecy, and data protection; and (2) to urge the Commission to include a ban on internet-connected voting machinery.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy issues.[2] The Association for Computing Machinery is the longest-established and largest association of individual professionals engaged in all aspects of computing in the world.[3] EPIC previously commented on the Voluntary Voting System Guidelines in 2009, stating:

> Ballot secrecy and voter privacy must be core values within the context of voting technology standards and testing and certification of voting systems [4]

---

[1] *Notice of proposed Voluntary Voting System Guidelines 2.0 Principles and Guidelines request for public* comment, 84 Fed. Reg. 6775-76 (Feb. 28, 2019), https://www.govinfo.gov/content/pkg/FR-2019-02-28/pdf/2019-03453.pdf.
[2] EPIC, *About EPIC* (2018), https://epic.org/epic/about.html.
[3] ACM engages in public policy through its U.S. Technology Policy Committee, to which participation in these comments should be attributed.
[4] EPIC, Comments Regarding the 2009 Voluntary Voting System Guidelines Version 1.1, Election Assistance Commission, 6 (Sept. 28, 2009), https://epic.org/privacy/voting/epic_eac_comments_10-09.pdf.

I. The Secret Ballot is Vital for Democracy

We applaud the draft VVSG's robust principles on voter privacy and ballot secrecy. The secrecy of the ballot is a foundation of our democracy. In 2016, EPIC, Verified Voting, and Common Cause released a report and fifty state survey on the issue of ballot secrecy. We found that a vast majority of states (44) have a constitutional provision guaranteeing secrecy in voting, while the six remaining states have statutory provisions referencing secrecy in voting.[5] The secret ballot is the kernel of democracy. "The secret ballot reduces the threat of coercion, vote buying and selling, and tampering. For individual voters, it provides the ability to exercise their right to vote without intimidation or retaliation."[6]

As the National Academy of Sciences recently found, "If anonymity is compromised, voters may not express their true preferences."[7] While advances in technology can facilitate voting in a variety of ways—voter registration, tracking ballots, finding poll places, checking wait times, etc.—current cyber security techniques cannot prevent the linking of an individual to his or her marked ballot when transmitted over the internet.[8] Thus digital voting techniques pose a real and ongoing risk in the specific area of vote tabulation.

EPIC and the USTPC urge the Commission to leave Principle 10: BALLOT SECRECY unchanged, ensuring that no direct or indirect identifiers can link the voter's identity with the "voter's intent, choices, or selections."[9]

II. Algorithmic Transparency is Key to Ensuring Accountability

Accountability is key to ensuring faith in our electoral process. As decisions are automated, and organizations increasingly delegate decision-making to techniques they do not fully understand, processes become more opaque and less accountable. It is therefore imperative that algorithmic process be open, provable, and accountable.

We commend the inclusion of guideline 13.3 – "All cryptographic algorithms are public, well-vetted, and standardized" and urge the Commission to leave the guideline unchanged.

III. The VVSG 2.0 must ban internet connectivity or the use of wireless modems in voting systems

The VVSG 2.0 draft is missing a requirement that is critical to election security: a ban on internet connectivity or the use of wireless modems in vote recording or vote tabulating systems. The current draft would allow voting machines to connect to the Internet, perhaps even through a wireless connection.

---

[5] Caitriona Fitzgerald, Pamela Smith, Susannah Goodman, *Secret Ballot at Risk: Recommendations for Protecting Democracy*, 1 (Aug. 18, 2016), http://secretballotatrisk.org/Secret-Ballot-At-Risk.pdf.
[6] *Id.* at 5.
[7] National Academies of Sciences, Engineering, and Medicine, *Securing the Vote: Protecting American Democracy* 87 (2018), https://doi.org/10.17226/25120.
[8] *Id.* at 4.
[9] Proposed Voluntary Voting System Guidelines 2.0 Principles and Guidelines at 4.

We urge the Commission to add a guideline under Principle 13: DATA PROTECTION:

> *"The voting system does not use wireless technology or connect to any public telecommunications infrastructure."*

As the National Academies of Sciences, Engineering, and Medicine stated in the 2018 Report on election security:

> At the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots. Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet.[10]

The National Academies concluded that "[s]ecure Internet voting will likely not be feasible in the near future."[11]

Computer scientists have long cautioned that Internet voting "not only entails serious security risks, but also requires voters to relinquish their right to a secret ballot."[12] After the 2016 election, cybersecurity expert Bruce Schneier wrote:

> We need national security standards for voting machines, and funding for states to procure machines that comply with those standards.
>
> This means no Internet voting. While that seems attractive, and certainly a way technology can improve voting, we don't know how to do that securely. We simply can't build an Internet voting system that is secure against hacking because of the requirement for a secret ballot. This makes voting different from banking and anything else we do on the Internet, and it makes security much harder. Even allegations of vote hacking would be enough to undermine confidence in the system, and we simply cannot afford that.[13]

---

[10] National Academies of Sciences, Engineering, and Medicine, *supra* note 7, at 106.
[11] *Id.* at 102.
[12] Douglas W. Jones and Barbara Simons, Broken Ballots: Will Your Vote Count? 291 (2012); Bruce Schneier, *By November, Russian hackers could target voting machines*, Washington Post (July 27, 2016), https://www.washingtonpost.com/posteverything/wp/2016/07/27/by-november-russian-hackers-could-target-voting-machines/; *Accord* Verified Voting, Computer Technologists' Statement on Internet Voting (September 2012), http://www.verifiedvoting.org/wp-content/uploads/2012/09/InternetVotingStatement.pdf; *see also* Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, *Security Analysis of the Diebold Accuvote-Ts Voting Machine Problems with Voting Systems and the Applicable Standards* (Sept. 2006), https://citp.princeton.edu/research/voting/; Peter G. Neumann, Security Criteria for Electronic Voting (1993), *available at* http://www.csl.sri.com/users/neumann/ncs93.html.
[13] Bruce Schneier, *Online Voting Won't Save Democracy*, The Atlantic (May 2017), https://www.theatlantic.com/technology/archive/2017/05/online-voting-wont-save-democracy/524019/.

Renowned cryptographer Ronald Rivest says that "best practices for internet voting are like best practices for drunk driving." – neither one makes sense.[14] Rivest says the dramatic loss of security with Internet voting does not outweigh the increased convenience for voters.[15]

Cyber security experts at the Department of Homeland Security and the National Institutes for Standards and Technology have warned against implementation of Internet voting in U.S. public elections because of privacy and security risks.[16] In July 2015, the U.S. Vote Foundation released a study establishing a new reference for security, usability and transparency standards necessary to implement Internet voting in public elections. Developed by the nation's leading experts in election integrity, election administration, high-assurance systems engineering, and cryptography, the study concluded that ***not one*** of the existing Internet voting systems provides adequate security for public elections or guarantees voter privacy.[17]

Washington DC's Internet voting pilot system was allowed to be tested before deployment. Researchers breached it with relative ease: "Within 36 hours of the system going live, our team had found and exploited a vulnerability that gave us almost total control of the server software, including the ability to change votes and reveal voters' secret ballot."[18]

Cybersecurity must be a top priority for the United States. We must protect democratic institutions against cyber attack by foreign adversaries. The Russian attacks on democratic institutions are expected to continue.[19] As the National Academies of Sciences, Engineering, and Medicine recently explained:

> The 2016 election vividly illustrated that hostile state actors can also pose a threat. These actors often possess more sophisticated capabilities and can apply greater resources to the conduct of such operations. Moreover, they may have other goals than shifting the outcome for a particular candidate. If their goal is to disrupt an election or undermine confidence in its outcome, they may need only to achieve DoS against e-pollbooks or leave behind traces of interference like malicious software or evidence of tampering with voter registration lists or other records. Even failed attempts at

[14] Christine Kane, *Voting and Verifiability: Interview with Ron Rivest*, Vantage Magazine (2010), https://people.csail.mit.edu/rivest/pubs/Kan10.pdf
[15] *Id.*; *see also* Ron Rivest, Auditability and Verifiability of Elections (March 2016), available at https://people.csail.mit.edu/rivest/pubs/Riv16x.pdf.
[16] Sari Horwitz, *More than 30 states offer online voting, but experts warn it isn't secure*, Wash. Post (May 17, 2016), *available at* https://www.washingtonpost.com/news/post-nation/wp/2016/05/17/more-than-30-states-offer-online-voting-but-experts-warn-it-isnt-secure/; *see also* National Institute of Standards and Technology (NIST), *Security Considerations for Remote Electronic UOCAVA Voting* (February 2011), *available at* http://www.nist.gov/itl/vote/upload/NISTIR-7700-feb2011.pdf; *and* Federal Voting Assistance Program, *2010 Electronic Voting Support Wizard (EVSW) Technology Pilot Program Report to Congress* (May 2013), *available at* http://www.fvap.gov/uploads/FVAP/Reports/evsw_report.pdf.
[17] U.S. Vote Foundation, The Future of Voting: End-to-End Verifiable Internet Voting - Specification and Feasibility Study (July 2015), *available at* https://www.usvotefoundation.org/E2E-VIV.
[18] Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman, *Attacking the Washington, D.C. Internet Voting System*, Proc. 16th Conference on Financial Cryptography & Data Security (Feb. 2012), https://jhalderm.com/pub/papers/dcvoting-fc12.pdf.
[19] Office of the Dir. of Nat'l Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections* (2017), 5, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

interference could, if detected, cast doubt on the validity of election results absent robust mechanisms to detect and recover from such attacks.[20]

The VVSG help shape the election security market. The Election Assistance Commission should not miss this critical opportunity to make a strong statement that elections and the Internet don't mix. The VVSG should add a guideline that bans internet connectivity or the use of wireless modems in vote recording or vote tabulating systems.

Conclusion

The VVSG 2.0 are vital to protecting our democratic institutions. The guidelines must ban the use of internet-connected voting machines and protect ballot secrecy.

Respectfully submitted,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

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

James A. Hendler
Chair, U.S. Technology Policy Committee of
the Association for Computing Machinery

[20] National Academies of Sciences, Engineering, and Medicine, *supra* note 7, at 92.