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

Testimony and Statement for the Record of

Caitriona Fitzgerald, EPIC Policy Director
Electronic Privacy Information Center

to the

Election Assistance Commission

Introduction and Foundation of VVSG 2.0 Requirements

March 27, 2020

Commissioners Hovland, Palmer, McCormick, and Hicks, thank you for the opportunity to testify today in support of the proposed Voluntary Voting System Guidelines (VVSG) 2.0 Requirements as submitted by the Technical Guidelines Development Committee.[1]

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] EPIC has long been interested in the technical standards for voting systems. EPIC previously commented on the Voluntary Voting System Guidelines in 2009 and followed closely developments ever since.[3]

Last May, EPIC and the U.S. Technology Policy Committee of the Association for Computing Machinery supported the proposed VVSG 2.0.[4] EPIC commended the inclusion of strong principles protecting voter privacy, ballot secrecy, and data protection; and urged the Commission to include a ban on internet-connected voting machinery. As we said at the time, "[t]he 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." We also highlighted the report of the National Academies of

---

[1] Election Assistance Comm'n Technical Guidelines Development Comm., *Recommendations for Requirements for the Voluntary Voting System Guidelines 2.0* (Feb. 29, 2020) https://www.eac.gov/sites/default/files/TestingCertification/2020_02_29_vvsg_2_draft_requirements.pdf [hereinafter "Proposed VVSG 2.0].

[2] EPIC, *About EPIC* (2018), https://epic.org/epic/about.html.

[3] 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 ("Ballot secrecy and voter privacy must be core values within the context of voting technology standards and testing and certification of voting systems.")

[4] *Comments of EPIC and U.S. Technology Policy Comm. of the Assoc. for Computing Machinery Regarding the Proposed Voluntary Voting System Guidelines 2.0 Principles and Guidelines* (May 29, 2019), https://epic.org/apa/comments/EPIC-USTPC-Comments-EAC-VVSG-May2019.pdf.

Sciences, which stated "If anonymity is compromised, voters may not express their true preferences."[5]

I. The Secret Ballot is Vital for Democracy

EPIC applauds the 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.[6] The secret ballot is the kernel of democracy.

EPIC strongly supports Principle 10: BALLOT SECRECY, ensuring that no direct or indirect identifiers can link the voter's identity with the "voter's intent, choices, or selections."[7]

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 the algorithmic process be open, provable, and accountable.

EPIC commends the inclusion of guideline 13.3 – "All cryptographic algorithms are public, well-vetted, and standardized" and urges the Commission to leave the guideline unchanged.[8]

III. Banning internet connectivity or the use of wireless modems in voting systems

EPIC supports the decision of the TGDC to make clear that voting systems must not be capable of establishing wireless connections or any connection to an external network.[9] 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."[10]

---

[5] National Academies of Sciences, Engineering, and Medicine, *Securing the Vote: Protecting American Democracy* 87 (2018), https://doi.org/10.17226/25120.
[6] 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.
[7] Proposed VVSG 2.0, *supra* note 1 at 24-25.
[8] *Id.* at 26.
[9] *Id.* at 254-255.
[10] Douglas W. Jones and Barbara Simons, Broken Ballots: Will Your Vote Count? 291 (2012); 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/; 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/; Ron Rivest, Auditability and Verifiability of Elections (March 2016), available at https://people.csail.mit.edu/rivest/pubs/Riv16x.pdf; *Accord* Verified Voting, Computer Technologists' Statement on Internet Voting (September 2012), Christine Kane, *Voting and Verifiability: Interview with Ron Rivest*, Vantage Magazine (2010), https://people.csail.mit.edu/rivest/pubs/Kan10.pdf;

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.[11] 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.[12]

Cybersecurity should be a top priority for the United States. We should protect democratic institutions against cyber attack by foreign adversaries. Recent reports from the Intelligence Community make clear that Russian attacks on democratic institutions are expected to continue.[13]

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 restrictions on internet connectivity and wireless connections in voting recording or vote tabulating systems in Principle 14 must be maintained.

IV. Conclusion

The VVSG 2.0 are vital to protecting our democratic institutions. The guidelines should prohibit the use of internet-connected voting machines and safeguard ballot secrecy. These standards are particularly important as the Commission and state election officials face the implementation of the 2020 U.S. Presidential Election amid the COVID-19 outbreak. It is crucial that Presidential election be held on schedule – our democracy depends on it – but we must do so while ensuring voter privacy, ballot secrecy, and election integrity.

---

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.

[11] 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.

[12] 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.

[13] 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.