

Last week, Free Speech For People forwarded two letters to the U.S. Election Assistance Commission (EAC) regarding the EAC's vote, scheduled for February 10, 2021, on the proposed federal Voluntary Voting System Guidelines (VVSG) 2.0. The letters addressed the EAC's decision to amend the draft VVSG 2.0 to permit wireless networking modems and chips in voting machines, provided they are disabled by software.

More than 20 computer security and election integrity experts opposed this change, warning that it was "recklessly naïve," would make voting machines vulnerable to remote cyber attacks, and corrode voter confidence in the election process. Further, Free Speech For People sent a letter charging that the EAC did an end-run around the VVSG development process prescribed in the Help America Vote Act (HAVA) of 2002.

In response, the EAC has issued a memo entitled "VVSG 2.0 Dispelling Misinformation," which attempts to distort the record and argue that the EAC did not significantly alter the draft that moved through the HAVA process. We find this memo to be little more than smoke and mirrors. The simple fact is the EAC *added language* to the draft VVSG 2.0 to explicitly state that the VVSG 2.0 will not ban wireless networking hardware. Had the original VVSG 2.0 draft allowed for wireless networking hardware, this statement would not have needed to be added. Furthermore, we believe that the record of discussions regarding this highly debated topic shows that the VVSG 2.0 should not permit the inclusion of hardware that is capable of making external network connections. At a December 2019 meeting of the TGDC a representative of the National Institute of Standards and Technology made these remarks in a presentation about wireless networking capability.

*"So, **the voting system itself would not have any wireless capability built into it** so you wouldn't be able to access its networking capabilities<sup>1</sup>...We would **remove that wireless capability** from the voting system like I mentioned, so there would be no wireless communication." [Emphasis added.]*

The EAC's memo is also profoundly troubling in that it describes what it would consider an acceptable configuration for voting systems that contain wireless networking devices.

*"...where the wireless subsystem uses a physical switch to control power and no drivers are present on systems that are in an active voting configuration."<sup>2</sup> [Emphasis added.]*

This seems to suggest that the mitigations to disable wireless connectivity via a power switch and a software configuration would only have to be in effect for "active" voting, allowing that the wireless networking *could* be enabled via switch and software configuration when the voting system is not engaged in an election session. For example, this seemingly could permit wireless networking before or after the polls close, for updates, election programming, or election night reporting.

The EAC's obligation to develop the VVSG and test and certify voting systems to these guidelines is a core responsibility and a central reason the Commission was created. The

---

<sup>1</sup> December 18, 2019 Meeting of the Technical Guidelines Development Committee. Available at: <https://www.youtube.com/watch?v=ycPX5yt0N-k&t=1745s> at 51:18 and 52:40

importance of this responsibility has only intensified in light of known attacks by foreign nation-state actors in the last two general election cycles. The importance of the EAC's task to provide voting systems which are both secure and trustworthy cannot be overstated. Weakening the federal standards to permit devices that could expose voting systems to exploitation is profoundly ill-advised at this time.