October 15, 2019

Dear Members of the Technical Guidelines Committee,

Thank you for your service on the Technical Guidelines Development Committee (TGDC). Our organizations share your commitment to the development of robust, meaningful guidelines for federally-certified voting systems through a process which is both transparent and trustworthy.

We write to you because it has come to our attention that the U.S. Election Assistance Commission refused to provide the Committee with access to the public comments submitted for the development of the federal Voluntary Voting System Guidelines (VVSG) during the recent meeting of the Committee. During the TGDC meeting, members requested to review the public comments to inform the discussion and better discharge their responsibilities to provide guidance for both the VVSG and VVSG requirements. The Commission's refusal to provide the comments concerns us because our organizations engaged our members and the public to encourage the submission of public comments on the VVSG. We believe their voices should be heard.

Our organizations, from across the political spectrum, cooperated specifically to request the inclusion of a ban on wireless modems and internet connectivity in the proposed VVSG 2.0 under Principle 13. The need for a ban on wireless modems and internet connectivity was considered so essential to the public that over 50,000 individuals submitted comments to the Commission asking it to include a ban in the VVSG 2.0. This level of engagement on the VVSG is unprecedented and demonstrates the overwhelming demand from the public that our voting systems not be exposed to unnecessary threat vectors. The Commission's decision not to provide the comments or adequately quantify the number of comments received during this process deprived the Committee of the fact that the public strongly backs a ban on connectivity in federally certified voting systems as the Committee contemplated including such a ban in the VVSG requirements.

We would be pleased to provide the full set of comments upon request. For simplicity, here is the standard comment that most people submitted:

> *I strongly support the draft Voluntary Voting System Guidelines (VVSG) and commend the robust principles and guidelines for software independence, auditability and ballot secrecy.*
>
> *Given the fact that our election systems are being targeted for interference through cyberattacks, it is imperative the VVSG also prohibit connectivity to the public Internet through wireless modems or other means.*
>
> *We want to ban modems in vote counting machines both to protect data and to prevent manipulation.*
>
> *Therefore, we urge the Commission to add the following to the guideline under Principle 13: DATA PROTECTION:*
>
> *The voting system does not use wireless technology or connect to any public telecommunications infrastructure."*

> *Indeed, eliminating wireless modems and internet connectivity will not guarantee our voting machines can't be manipulated or hacked through corrupted USB sticks, insider attacks or supply chain corruption. That is why ultimately all votes should be cast on paper ballots and all elections should be audited by manually counting a sample of the paper ballots, but this guideline is essential while we still use voting machines.*

The Commission's failure to adopt the recommendations and include a ban on wireless modems and internet connectivity in the VVSG is especially puzzling given that it has frequently made false or misleading statements to the public[1] and to Congress[2] that the current VVSG do, in fact, ban internet connectivity. The Commission misled the public to believe the VVSG does include this important safeguard, yet ignored the public request to include this provision in the VVSG.

As you consider this important topic, we would also bring to your attention a recent news article in which security researchers identified many election management systems connected to the internet, often for months, with visible security issues. Jurisdictions were unable to provide adequate oversight and were prevented, often by law, from upgrading software to address known, critical vulnerabilities. If the VVSG allows voting systems to connect over public telecommunications networks, it cannot protect them from these and other inherent risks because its scope is limited to the voting system hardware and software. At the same time, the current threats to our elections have magnified the risks of using public networks to levels the Committee has not previously contemplated.

The Committee has wisely acknowledged that public confidence in the election process is critical. Prohibiting connectivity will provide both better security and better confidence in the election process. As the Committee continues its vital work on the VVSG requirements we believe it is essential that the Committee be aware of the strong public sentiment for a ban on internet connectivity in federally certified voting systems and reconsider including a ban on connectivity in the VVSG requirements.

Thank you for your consideration of this information. We stand ready to assist the Committee in any way necessary and would be happy to answer any questions you may have.

Sincerely,

National Election Defense Coalition

FreedomWorks

OSET Institute

SMART Elections

Public Citizen

[1] Tom Hicks, Matt Masterson, Christy McCormick "Don't believe the hype. Foreign hackers will not choose the next president," *The Washington Post,* Oct. 18, 2016

[2] In testimony at the May 15, 2019 hearing of the Senate Rules Committee, Commission Chair Christy McCormick stated "the VVSG does not allow for internet connectivity." https://www.youtube.com/watch?v=6NcndQmG9BE at 3:35.