February 3, 2021

Chairman Benjamin Hovland
Vice Chair Donald Palmer
Commissioner Tom Hicks
Commissioner Christy McCormick
U.S. Election Assistance Commission
633 3rd Street NW, Suite 200
Washington, DC 20001

Dear Chair Hovland, Vice Chair Palmer, Commissioner Hicks and Commissioner McCormick,

We, as members of the computer science, cybersecurity, and election integrity communities, are writing to strongly discourage the U.S. Election Assistance Commission (EAC) from permitting the inclusion of disabled wireless radios, wireless chips, modems and/or hardware capable of connecting election systems to public telecommunication infrastructure, including the Internet, in the next version of the federal Voluntary Voting System Guidelines (VVSG 2.0), to be voted on February 10th. This would be a grave mistake as it would significantly increase the potential for remote cyber-attacks on voting systems, and would corrode public confidence in our election systems and institutions.

During the 2016 election cycle, Russian intelligence agents remotely gained and maintained access to State and County board election networks.[1] Public concerns about the security of our election infrastructure are higher than ever before. It is crucial that our election systems be secure, and that our citizens trust that election systems are secure. Permitting the inclusion of wireless radios will both increase the vulnerabilities of the voting system and diminish voter confidence in the security of our election systems. Neither is acceptable.

The draft requirements for the VVSG 2.0 developed by the Technical Guidelines Development Committee (TGDC), and affirmed by the Standards Board and Board of Advisors, in compliance with requirements in the Help America Vote Act of 2002, do not permit the inclusion of devices capable of connecting voting systems to networks wirelessly.

Principle 14 of the draft VVSG 2.0 delivered to the EAC by the TGDC protects system integrity through specific guidelines under principle 14. Guideline 14.2 clearly requires that:

> *14.2 - The voting system limits its attack surface by avoiding unnecessary code, data paths, connectivity, and physical ports, and by using other technical controls.*

This is further elucidated in guideline 14.2.D which specifies that voting systems *must not include the capability to establish wireless connections*.

> ***14.2-D – Wireless Communication Restrictions***

[1] "Assessing Russian Activities and Intentions in Recent US Elections," Office of the Director of National Intelligence, January 6, 2017. *Available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf*

> *Voting systems **must not be capable** of establishing wireless connections.[Emphasis added.]*

As the VVSG 2.0 was being drafted, this issue was considered exhaustively by the TGDC and the National Institute of Standards and Technology (NIST), which is responsible for chairing the TGDC and providing technical guidance for the development of the VVSG. NIST also provided detailed presentations on the use of wireless technology to the EAC's Board of Advisors and Standards Board to inform members of the concerns and considerations before each body voted to accept the draft VVSG 2.0 with the wireless prohibition.

On February 1, 2021, the EAC published a new draft VVSG 2.0 slated for consideration by the Commissioners on February 10th. This new draft is drastically different from the version that was developed by the TGDC, and approved by the Board of Advisors and Standards Board. The new draft will allow voting systems with internal wireless radios, chips, modems and/or hardware capable of wireless networking, provided the wireless connectivity is not enabled. We understand the EAC is considering this position at the urging of voting system vendors, citing the desire to build systems with commercial-off-the-shelf (COTS) computerized tablets and scanners which may be sold with wireless networking capability. **While this may seem to provide certain cost advantages, it profoundly weakens voting system security and will introduce very real opportunities to remotely attack election systems. Therefore, we strongly advise you to maintain a prohibition on wireless networking capability in the VVSG 2.0.**

A voting system that includes networking capability would have all of the hardware *and* software necessary for making incoming or outgoing network connections - meaning they would be one software configuration away from being remotely accessible, and potentially remotely attacked. If wireless networking capability is there, it is *inevitable* that it will get turned on and used. It would be a recklessly naïve mistake to expect that procedures and processes could ensure that the wireless capability could or would not be activated, intentionally or unintentionally.

Wireless networking capability can easily be enabled unintentionally through a misconfiguration, a software update, or a technical error. It's not difficult to imagine a warehouse worker enabling the network features for an operation and then forgetting to turn it off on every machine. Furthermore, the wireless capability in many COTS devices will likely be enabled by default at the time of booting. Such machines would have to be *deliberately* reconfigured after booting, which could be easily overlooked, or the Operating System will have to be specifically altered to disable wireless capability by default during booting. And even if a wireless application is disabled, the networking hardware may remain enabled. This is not theoretical supposition. In 2015, the Virginia Department of Elections decertified the WINVote voting machine after commissioning a security review of the WINVote by Virginia's Information Technologies Agency (VITA) which found the machines could be wirelessly accessed and manipulated. In its security assessment VITA wrote:

> *"**One additional important note is that while the WINVote application appears to have the ability to disable the wireless network from within the application, it does not disable the network interface on the device.** When the wireless network is disabled using the WINVote interface, the application will no longer seek other devices on the network. Although the application will not find other systems, the device's network card remains*

> *online and will send and receive traffic even though the application indicates it is disabled."*[Emphasis added.][2]

The WINVote's susceptibility to remote manipulation via its wireless capability caused the Commonwealth to hastily decertify it before a major election. That the EAC would seek to permit the same type of vulnerability in the federal voting system guidelines six years later indicates a distressing lack of knowledge about election system security.

Even if election officials consistently disable wireless capability during an election, officials or vendors will likely use wireless connectivity during warehouse maintenance for software upgrades or during configuration for an election. During those times the machines will be vulnerable to attempted remote penetration attacks. Connecting to the Internet, even briefly during machine maintenance, programming, pre-election testing, poll worker training, or on Election Day, makes the system vulnerable to attacks that could impact current or future election results. When contemplating the use of wireless modems and connectivity to public networks in the next generation of the federal voluntary voting system guidelines, NIST wrote:

> *"There are significant security concerns introduced when networked devices are then connected to the voting system. This connectivity provides an access path to the voting system through the Internet and thus an attack can be orchestrated from anywhere in the world (e.g., Nation State Attacks). The external network connection leaves the voting system vulnerable to attacks, regardless of whether the connection is only for a limited period or if it is continuously connected."*[3]

A successful penetration attack could allow one infected machine in the warehouse to perhaps infect all the others nearby whose modems are on the same penetration exploit that was used on the first one, creating a wireless worm.

Warehouse workers typically carry WiFi and cellular devices in their pockets, creating an exploitable attack vector. A capable hacker could attack one of the election workers' cell phones first, and use it as a springboard to attack nearby voting systems whose modems happen to be on.

We also cannot discount the possibility that the wireless networking capability could be enabled intentionally, by malware, a malicious actor, or an insider aiming to exploit the capability and remotely access and undetectably tamper with the system functionality or data, or both. As we learn more about the devastating attack on our networks via SolarWinds and Microsoft, we cannot discount the possibility of malicious bugs or backdoors in underlying operating systems.

Permitting the inclusion of wireless connectivity capability in federally certified voting systems will also allow vendors to game VVSG certification. Vendors could certify a system contingent on the wireless capability being disabled, knowing that post-certification they can flip a switch to provide wireless connectivity for states or counties that prefer it. Allowing wireless networking

---

[2] "Security Assessment of WinVote Voting Equipment For Department of Elections." Virginia Information Technologies Agency, April 14, 2015. *Available at: https://www.wired.com/wp-content/uploads/2015/08/WINVote-final.pdf*

[3] "Draft Recommendations for Requirements for the Voluntary Voting System Guidelines VVSG 2.0," National Institute of Standards and Technology, January 31, 2020. *Available at*: https://collaborate.nist.gov/voting/pub/Voting/VVSG20DraftRequirements/vvsg-2.0-2020-01-31-DRAFT-requirements.pdf

capability as a latent feature makes it easier for vendors to engage in this inadvisable practice and will improperly give state and county officials the false impression the EAC certified the wireless capability. These concerns are not speculative; as you know, the nation's largest voting system vendor, ES&S, was sanctioned for improperly advertising its voting systems with wireless modems as federally certified when they were not.[4]

Vendors may be lobbying to allow wireless networking hardware in voting systems in the VVSG 2.0 with the argument that this would permit the use of more COTS devices and reduce voting system costs overall, but we find this argument specious. The COTS devices that can be used in voting machines are not consumer-grade devices like iPads and Surface Pros. Instead, vendors use screens by non-retail companies like AValue. These non-consumer devices are typically *less expensive* precisely because they leave out extra, unnecessary features like wireless radios. Devices without wireless are available and vendors can choose them over more expensive wireless-enabled consumer-grade products. (E-pollbooks use consumer COTS devices, but are not in scope of the VVSG and therefore not relevant to this discussion.)

Merely requiring the system to provide notification that the wireless is enabled (as contemplated in the draft VVSG 2.0 requirements) is woefully insufficient as a security measure because any competent cyber-attack would easily direct the device to lie and not disclose that it is connecting to public networks.

Finally, and perhaps most importantly, in order to foster public trust in our election systems, wireless networking should be strictly prohibited in all voting systems. Including wireless networking capacity will only foster public distrust. This runs counter to our shared goal of increasing public trust in elections by providing trustworthy election technology. Permitting the inclusion of wireless networking capability to facilitate system programming, software updates and maintenance via wireless networking is profoundly ill-advised and unacceptably insecure for voting systems in today's threat environment.

We strongly urge the EAC to ensure the VVSG 2.0 reflects the provisions in the principles and guidelines as drafted by the TGDC, which prohibit voting systems from including the *capability* of connecting wirelessly to public networks. The VVSG 2.0 should either ban the inclusion of wireless networking devices in voting systems, or should require the wireless networking devices be *physically* disabled.

Prohibiting the inclusion of wireless radios in voting systems will not make voting systems impenetrable. Many other attack vectors still exist. The only way to ensure resilience in voting systems is by requiring voter-verified paper ballots, verifiably secure chain of custody of the ballots, and robust, manual post-election audits of the results against the paper ballots.

The undersigned thank you for your service and your immediate attention to this critical national security issue. We stand ready to work with you to protect our nation's election infrastructure from all threats, foreign and domestic.

Sincerely,

[4] Kim Zetter, "Election commission orders top voting machine vendor to correct misleading claims," *Politico,* August 13, 2020. *Available at: https://www.politico.com/news/2020/08/13/election-voting-machine-misleading-claims-394891*

Dr. Andrew W. Appel
Professor of Computer Science
Princeton University*

Dr. Elisa Bertino
Samuel Conte Professor of Computer Science
Cyber2SLab, Director
Computer Science Department
Purdue University*

Dr. Elizabeth Bradley
Professor
University of Colorado Boulder*

Dr. Duncan Buell
Chair Emeritus — NCR Chair in Computer Science and Engineering
Dept. of Computer Science and Engineering
University of South Carolina*

Lowell Finley
former Deputy Secretary of State
California

Dr. Richard A. DeMillo
Charlotte B. and Roger C. Warren Professor of Computer Science
College of Computing
Georgia Institute of Technology*

Dr. Kathleen Fisher
Professor and Chair, Computer Science
Tufts University*

Susan Greenhalgh
Senior Advisor on Election Security
Free Speech For People

Dr. J. Alex Halderman
Professor, Computer Science and Engineering
Director Center for Computer Security and Society
University of Michigan*

Harri Hursti
Founding Partner Nordic Innovation Labs and Election Integrity Foundation*

Dr. David Jefferson
Lawrence Livermore National Laboratory*
(retired)

Dr. Douglas W. Jones,
Associate Professor of Computer Science,
University of Iowa*
Former member, Technical Guidelines Development Committee

Dr. Helen Nissenbaum, Professor
Director, Digital Life Initiative
Cornell Tech, New York City*

Dr. Peter G. Neumann,
Chief Scientist,
SRI International Computer Science Lab*

Mark Ritchie
Former MN Secretary of State
Member of the EAC Board of Advisors*
Former president of the National Association of Secretaries of State*

Dr. Avi Rubin
Professor, Computer Science
Johns Hopkins University*

Bruce Schneier
Fellow and Lecturer
Harvard Kennedy School*

Kevin Skoglund
Chief Technologist
Citizens for Better Election*

Professor Eugene H. Spafford
Executive Director Emeritus, CERIAS
Purdue University*

Dr. Philip B. Stark
Professor of Statistics
Associate Dean, Division of Mathematical and Physical Sciences
University of California, Berkeley*

Dr. Poorvi L. Vora
Professor of Computer Science
The George Washington University*

Dr. Ellen W. Zegura
Fleming Professor, School of Computer Science
Georgia Institute of Technology*
Chair, Computing Research Association

*Affiliations listed are for identification purposes only and do not imply institutional endorsement.

cc. U.S. Senate Committee on Rules & Administration
Committee on House Administration