FREE SPEECH FOR PEOPLE.ORG

June 7, 2023

Chair Christy McCormick
Vice Chair Benjamin Hovland
Commissioner Tom Hicks
Commissioner Don Palmer
U.S. Election Assistance Commission
633 3rd Street NW, Suite 200
Washington, DC 20001
Attn: Testing & Certification

Submitted electronically

RE: Comments on VVSG 2.0

Dear Chairman McCormick and Commissioners,

We[1] thank the Commission for adopting this policy to provide additional feedback on the Voluntary Voting System Guidelines 2.0 (VVSG 2.0), and write to provide public comment on the VVSG 2.0.

Two of the primary responsibilities the U.S. Election Assistance Commission (EAC) was charged with at its inception are the development of the VVSG and certifying voting systems to those standards. In 2016, when U.S. intelligence agencies warned us that the foreign adversaries were targeting our election infrastructure with cyber attacks, the EAC's charge to develop voting system standards and certify our election systems took on unprecedented

[1] Free Speech For People is a non-profit, non-partisan public interest legal organization that works to renew our democracy and our United States Constitution for the people. As part of our mission, we are committed to promoting, through legal actions, secure, transparent, trustworthy and accessible voting systems for all voters.

importance. The EAC is responsible for creating guidelines for the mission-critical operation which underpins the legitimacy of our self-governing democracy. Indeed, in appearances before Congress the EAC Commissioners have frequently defended the EAC's relevance by highlighting these duties. Their importance to our national security cannot be overstated.

We submit comments on several issues that we believe should be addressed in the VVSG 2.0, and then provide, specific inline recommendations that we believe would improve the clarity and efficiency of the VVSG 2.0.

1. Penetration Testing

The current EAC Testing and Certification Manual 3.0 calls for penetration testing of voting systems. This is an important security tool and we support this measure and agree it's an important step forward toward more secure election systems.

However, penetration testing, as it's being employed by the testing and certification process is deeply flawed and drained of any benefit. The manual specifically states this will not be open-ended vulnerability testing, placing clear limits on the testing. Moreover, the penetration testing is not a part of the VVSG 2.0, the tests and results are not public, and there are no requirements to remedy security vulnerabilities that may be uncovered in the process of the penetration testing. In other words, penetration testing may reveal severe security vulnerabilities, but as long as a system conforms to the VVSG 2.0 requirements and test assertions, it can receive full EAC Certification. Further, there is no mechanism through the testing and certification program to pressure vendors to remedy the vulnerabilities before a system version is upgraded, so these vulnerabilities may persist from version to version of a voting system that is certified.

These deficiencies are compounded by the fact that penetration testing is often cited by the EAC and voting system vendors as a benefit to the testing and certification program to improve voting system security. This significantly overstates the influence penetration testing will actually have on voting systems that get certified, which is effectively none.

We strongly urge the EAC to reassess and revise the penetration testing provision in the Testing and Certification Manual to effectively utilize this important security tool, and to include requirements that vendors effectively remediate severe security vulnerabilities that are discovered.

2. Wireless networking capability

The version of the VVSG 2.0 that was a published for public comment in 2020 reflected the conclusions of the VVSG Cybersecurity working group, and the National Institute of Standards and Technology (NIST), specifically that the voting systems must not be capable of establishing wireless connections. This was specified in Requirement 14.2.-D, Wireless Communication Restrictions, which states, "Voting systems must not be capable of establishing wireless connections." Requirement 14.2-E, External Network Restrictions, reenforced the requirement, by mandating, "A voting system must not be capable of... 1. establishing a connection to an external network; 2. connecting to any device that is capable of establishing a connection to an external network." This text was approved by the Technical Guidelines Development Committee, the Board of Advisors, and the Standards Board, as required by the Help America Vote Act of 2022.

The EAC subsequently changed this language and intent, outside of the process mandated by the Help America Vote Act (HAVA) of 2002, by adding language that explicitly permits including wireless networking devices in voting systems. This introduces wireless networking capability.

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,*

[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*

> *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 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]

There may be arguments made to allow wireless networking hardware in voting systems in the VVSG 2.0 on the basis 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

[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

[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*

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 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.

3. <u>Advertisements on ballots</u>

The VVSG 2.0 should include a provision that prohibits voting system vendors from advertising their products on ballots.

4. <u>Public inspection of End to End (E2E) Verifiable Protocols</u>

As the EAC and NIST approach the complicated task of vetting and approving E2E protocols, this process should be fully public and transparent. We strongly urge the EAC to require all E2E protocols submitted for certification to be made posted and available for public assessment for a minimum of two years.

5. Specific Comments to the VVSG 2.0

Introduction: With respect to the VVSG 2.0 Introduction, in our comments submitted in 2020, we recommended adding this sentence to the first paragraph on page 11, "*Issues of ballot secrecy can be substantially ameliorated by adopting ballot marking devices that produce a marked paper ballot identical in format and size to pre-printed paper ballots.*"

We renew this comment. Ballot marking devices (BMDs) that produce a ballot that does not resemble pre-printed ballots marked by pen create the ballot secrecy issue described. It is appropriate to note that this problem can be ameliorated or avoided entirely by employing BMDs that provide a ballot that resembles a pre-printed ballot.

In the same section, the VVSG 2.0 introduction includes the phrase: "*and may not be sufficient to provide equal access as required by law.*"

This contradicts a citation from HAVA earlier in the Introduction, which states that one accessible device is sufficient. Furthermore, the EAC has not supplied a legal analysis in support of this assertion. We recommend deletion of that phrase.

In this same section, the VVSG states: "*To support best practices, states should consider legislation and additional resources to ensure balanced access to accessible voting machines wherever voting technology is deployed and used for elections.*"

The VVSG 2.0 should not recommend to legislation to states. This is out of scope for the VVSG and should be deleted.

Section 1.1.2
Recommended addition: "*1.1.2 M -Logic and accuracy testing functions shall not rely upon any test data stored within the device or subsequently installed electronically into the voting device such as a test pattern.*"

This addition is recommended to prevent "auto test" features promoted by vendors which are insufficient and failed to detect programming errors that resulted in incorrect election results in the November 2019 election in Northampton, Pennsylvania.[5]

Section 1.1.5
Recommended Addition: "*1.1.5- B An electronic ballot marker may only record contest selections on a paper ballot sheet and may not record, store or export electronic copies of any contest selection*."

Electronic ballot markers should not be capable of electronically recording votes; systems which record votes electronically should be classified as Direct Record Electronic.

Section 1.1.5 -I
Recommended addition: "*Vote choices recorded on paper should be in human readable form.*"

Recording vote choices in barcodes creates a non-verifiable record of votes used for counting. Even if the vote choices are also recorded in human readable text, the scanners are counting a record that was not verified by the voter. Even if the election results are robustly audited, studies have shown the voters do not adequately verify the vote selections to provide a reliable audit record. Ballots produced by ballot marking devices should be designed to produce ballots that are identical in format to pre-printed ballots.

Section 1.1.9 L
Recommended addition "*If ballots are processed in a central-count operation by batch, the election system must have capability to create a report of the totals of the votes in the contests included in each batch, such that it can be prepared prior to any random draw of a batch-comparison audit.*"

This will facilitate certain methods of post-election audits.

[5] Nick Coransiniti, "A Pennsylvania County's Election Day Nightmare Underscores Voting Machine Concerns," *The New York Times,* November 30, 2019. *Available at:* https://www.nytimes.com/2019/11/30/us/politics/pennsylvania-voting-machines.html

Section 3.3-D
Recommended deletion: "*The voting system must be capable of producing a report on an election-by-election basis to show the meaning of codes and other data used within barcodes and CVRs to represent ~~ballot selections and~~ ballot style information.*"

Vote selections should not be encoded in non-human readable form for scanning and counting.

Section 2.5.1 -D
Recommended addition: *"Voting systems must also not have "back doors" such as bootable USB Drives where an attacker might insert a drive and take over the voting system."*

Section 3.1.1.-E
Recommended addition: "*Expected values for confirmed digital signatures of procured software components should be attached to the declaration.*"

A declaration from the manufacturer that software items were obtained directly from the manufacturer or distributor is insufficient. The digital signature and its expected value should be included.

Section 3.1.2-B
Recommended add after section 3.1.2-B "*The maximum voting rate for electronic ballot markers (BMD) must be documented to include setup time between voters, time for an average voter to mark a ballot of specified complexity, and the time necessary for an average voter to verify the resulting selections if that must be completed before leaving the BMD.*"

Section 7.1-I
Recommended addition: "*Font and layout on paper should support potential use of optical character recognition on ballot images for use as an alternative means of tabulation or supplemental audit review.*"

Many ballot marking devices print ballot summary cards with a font size too small for voters to read and verify.

Section 8.3-A
Recommended adding point "*3. In particular, they must report the rate at which voters detect and report discrepancies with BMD printed ballots purposely misprinted during the usability test.*"

News reports indicate voters have found errors in the printed ballot summary produced by a BMD.[6] It's essential to also track such errors in usability tests.

Section 9.1.5.-F
Recommended addition at the end: *"…not seen by the voter or anyone in the presence of the voter*."

The unique ballot identifier generated to facilitate audits should not be known to the voter, or anyone.

Section 14.3-C
Recommended change: replace "*critical*" with "*every component in the system*."

The Bill of Materials must not be limited to critical components as non-critical components may factor into malfunctions or contain security vulnerabilities that impact the entire system.

Thank you for the opportunity to submit comments on the VVSG 2.0. If you have any questions or require more information, please don't hesitate to contact me.

Sincerely,

Susan Greenhalgh
Senior Advisor for Election Security
Free Speech For People
susan@freespeechforpeople.org

[6] Will Peebles, "How Covid-19 wreaked havoc on Georgia, Chatham County elections process," *Savannah Morning News,* June 12, 2020. *Available at: https://www.savannahnow.com/news/20200612/how-covid-19-wreaked-havoc-on-georgia-chatham-county-elections-process*