United States Election Assistance Commission

Dispelling Misinformation about VVSG 2.0

The VVSG 2.0 is a much-needed strengthened set of enhanced security requirements for voting machines.

- The EAC worked closely with National Institute of Standards and Technology (NIST), (two-hour meetings twice weekly) to clean up the VVSG 2.0 language to remove redundancies and improve clarity.
- The EAC hosted regular internal meetings throughout the year with commissioners, staff, and EAC contractors to work through the VVSG 2.0 in preparation of the long-awaited scheduled February 10th vote by the Commissioners.
- The EAC worked diligently with NIST along with an internal EAC working group composed of EAC staff to conduct conversations with numerous stakeholders during the comment resolution period to clarify comments that various parties made (manufacturers, laboratories, election officials, etc.). The EAC engaged with manufacturers a few times during that period. This was a normal part of the comment resolution process and necessary for the EAC and NIST to complete their work. Manufacturers did not have veto power over any requirements, nor were the limited meetings, for the purpose of clarification, seeking consensus from manufacturers and no one was permitted to provide additional comments outside of the public comment period. It was critical that the EAC request clarification from manufacturers since they testified, they had feasibility concerns regarding building machines to VVSG 2.0 in an EAC public meeting and it was not clear what the precise technical issues were.
- The EAC hosted 3 public meetings on the VVSG 2.0, (see timeline below).
- The EAC reviewed and resolved all VVSG comments.
- The EAC did not dramatically alter the requirements including the Wireless section 14.2-C, as seen in the comparison chart below, the intent all along was disabling the wireless, (see section 15-.4-C) in the version posted from March 24, 2020.
- The EAC followed the required process in accordance with HAVA including but not limited to Section 222 of the Help America Vote Act (HAVA), 52 U.S.C. § 20962.
- The EAC allowed an opportunity for public input via publication of **notice of the proposed guidelines** in the Federal Register, an opportunity for public comment on the proposed guidelines, an opportunity for a public hearing on the record.
- The EAC intends to publish **the final requirements** and guidelines once the Commissioners vote on the VVSG 2.0. Until this vote, the VVSG 2.0 is a draft.
- The EAC Commissioners are voting on February 10th on the Guidelines and Requirements that were developed and approved by the Technical Guidelines Development Committee (TGDC), subject to numerous public hearings, approved by the Standards Board and modified based on public comment.

Timeline- The EAC followed the process in HAVA

- ✓ Sept. 19-20, 2019 TGDC Meeting on the VVSG 2.0
- ✓ Dec. 18, 2019 TGDC call to address accessibility and security issues, NIST presented on the VVSG 2.0 and specifically presented on disabling of the wireless, without any objections on the record.

- ✓ Feb. 7, 2020 Recommendation of the VVSG 2.0 Requirements are passed unanimously by the TGDC.
- ✓ March 9, 2020 The recommended requirements developed with the support of the NIST were submitted to the EAC's Acting Executive Director.
- ✓ Mar. 11, 2020 The EAC submitted the proposed VVSG 2.0 Requirements to the Standards Board and Board of Advisors executive committees for review.
- ✓ Mar. 24, 2020 VVSG 2.0 Requirements submitted for public comment.
- ✓ Mar. 27, 2020 Public hearing on the Introduction and Foundation of Voluntary Voting System Guidelines 2.0 Requirements.
- ✓ May 6, 2020 Public hearing on the VVSG 2.0 Requirements Hearing 2: Implementation of the VVSG at the State and Local Level.
- ✓ May 20, 2020 Public hearing on the VVSG 2.0 Requirements Hearing 3: Manufacturers & Voting System Test Labs
- ✓ June 16, 2020 Board of Advisors annual meeting discussed the VVSG 2.0.
- ✓ June 22, 2020 Public comment period closes.
- ✓ July 31, 2020 Standards Board meeting voted to approve the draft VVSG 2.0 with Requirements.
- ✓ Jan. 26, 2021 EAC notices in the Federal Register a vote on the VVSG 2.0 Principles and Guidelines and Requirements for February 10, 2021.
- ✓ Jan. 29, 2021 The EAC published the proposed VVSG 2.0 Requirements on eac.gov.

Wireless Section Explanation

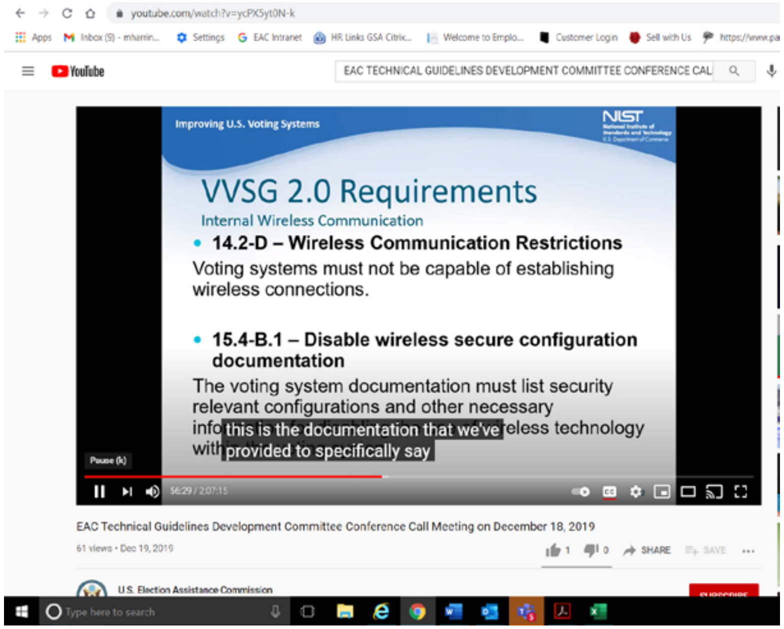
- The wording in the VVSG 2.0 draft that was published on Friday, January 29th, does not diverge dramatically from the recommended wording forwarded to the EAC from our boards.
  - This work was based on feedback received during the public comment period.
  - The draft we received from our boards did not mention a ban on wireless hardware that the EAC subsequently removed.
  - We worked with NIST to clarify the language to the discussion section on ways that wireless may be disabled and prevented from operating within a voting system. The language in the discussion section was provided by NIST after discussions with EAC staff.
    - The sentence within the discussion area that states: "This requirement does not prohibit wireless hardware within the voting system…" was added for clarity given the original intent was not to ban wireless as instructions of how to disable wireless were in the requirements approved by the TGDC and Standards board and posted for public comment.
    - It also recognizes the increasing difficulty in obtaining commercial off-the-shelf (COTS) components that do not contain this functionality in an attempt to not "paint ourselves into a corner" where voting system costs may rise substantially in the future if they require custom COTS configurations that are no longer widely available.
  - The added language goes beyond "airplane mode" and requires that wireless functionality not exist, whether

through not including the necessary hardware and/or removing any drivers or other software that could be used to enable it.

  - Wireless is effectively banned as any voting machine seeking to install the drivers, configure the hardware, and enable the functionality will not be certified by the EAC, and subsequently any jurisdiction or manufacturer enabling the functionality will be subject to a revoked certification.
  - If the EAC added language specifically prohibiting wireless hardware, our laboratories would be obligated to confirm this during certification testing. That may require them to view internal components of a COTS device, to confirm the absence of the hardware. We did not see a practical way to achieve this without relying solely on COTS manufacturer documentation of a component's features. Sometimes there are instances of undocumented hardware within COTS devices that are not advertised or enabled in certain models but may nonetheless still exist.
- In the public comments received, most comments supported leaving the requirement as-is, which we did.
  - There was a single comment from a manufacturer (Smartmatic, who only has machines deployed in LA County) mentioning that this restriction might cause issues for counties who rely on transmission of unofficial results due to geographic limitations. The VVSG 2.0 expressly prohibits this in EAC-certified systems.
    - We encourage manufacturers to develop novel ways to provide this functionality to their customers that does not introduce unacceptable vulnerabilities to certified systems.
- The VVSG 2.0 draft was developed with a "defense-in-depth" approach that does not rely on a single type of requirement (such as banning wireless) to achieve its security goals.
  - A major feature of VVSG 2.0 is the concept of "software independence". This requires voting systems to produce independently voter verifiable records (typically paper) that cannot be changed through an alteration to the system without providing warning/evidence that this has occurred.
  - Other compensating controls include requiring strong encryption or digital signing of data in transit and at rest within the system, source code quality control and review, user access control and the use of multi-factor authentication for critical operations, and mechanisms to prevent unauthorized software from executing.
  - Additionally, our updated Testing and Certification manual adds penetration testing as part of the process employed by our labs during certification testing as an additional layer to ensure that unknown vulnerabilities do not exist.
  - The program manual requires that manufacturers must "submit the final TDP of the voting system submitted for testing including all product bills of material, assembly drawings and schematics for the version being certified." The Testing Assertions which align with the Requirements, require documentation from the manufacturer to verify disabling of the wireless chipset through subsystem power control.
  - We have implemented a blend of mitigation controls to manage risk when complete elimination of wireless hardware is unattainable. Specifically, the combination of mechanisms (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), minimizes the effect of both unintentional and intentional failures. This configuration coupled with a robust Verification program enforces a persistent 'defense- in- depth' approach through the lifecycle of a voting system. We have verified this assessment through an independent expert cyber security firm. We believe we have dramatically enhanced security with the safeguards we mention above. The specific wireless attack vector with these safeguards is mitigated.

- Wireless was intended to be disabled in the VVSG 2.0 as seen in the Dec. 18, 2019 presentation from NIST to the TGDC, as well as can be seen in the VVSG 2.0 requirements document that was posted in March, (see screenshot below).
- Removing the hardware was not a requirement in the requirements posted on March 24, 2020, see screenshot below of 15-4.C requirements **on how to disable wireless, if the intent was for a complete ban requiring no hardware present, information on disabling wireless would not have been included in the requirements draft placed out for public comment.**
- During discussions with election officials and the Boards, concerns were raised regarding a complete ban on wireless due to accessibility concerns, and other election administration practices.
- We hope to see manufacturers build machines without the wireless hardware, as we have seen in the VVSG 1.0. These requirements are based on the possibility that the elimination of the wireless hardware is unattainable in some circumstances.



VVSG 2.0 Requirements

Internal Wireless Communication

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

Voting systems must not be capable of establishing wireless connections.

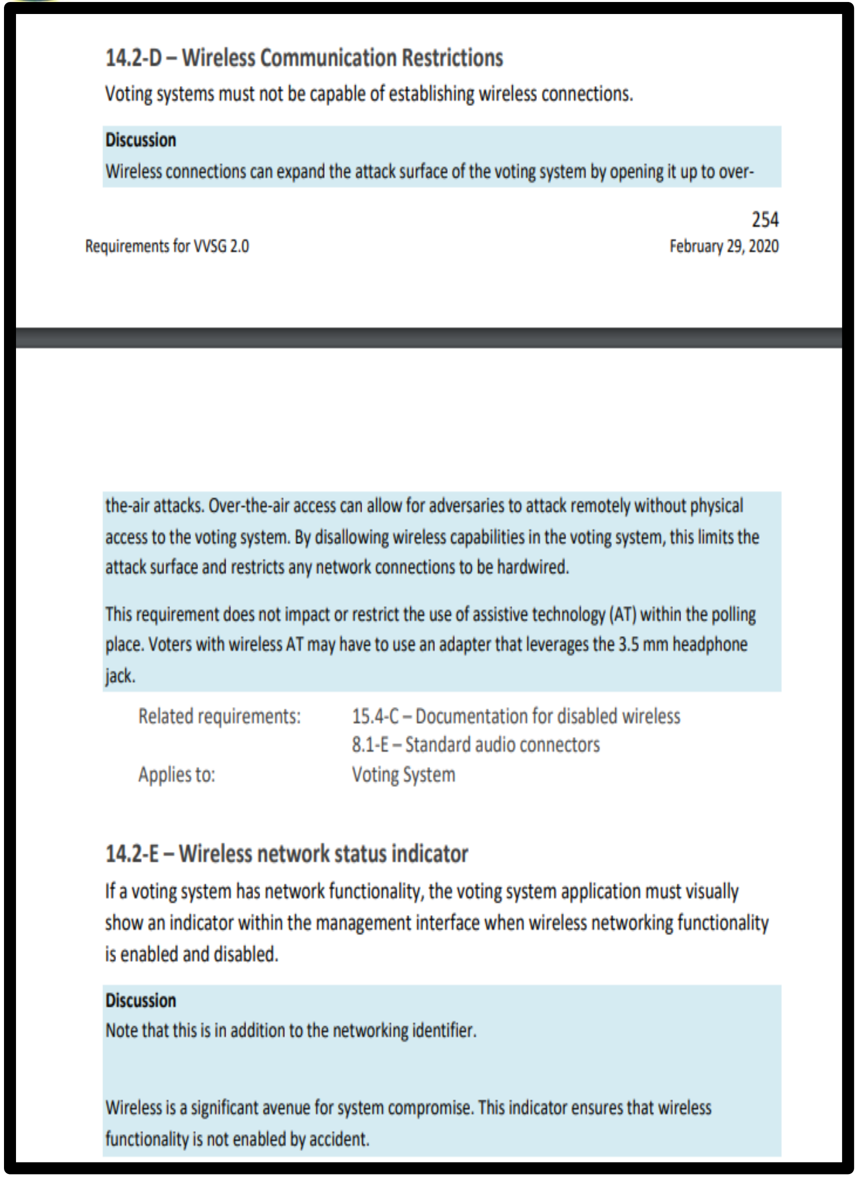
- **15.4-B.1 – Disable wireless secure configuration documentation**

The voting system documentation must list security relevant configurations and other necessary info this is the documentation that we've eless technology with provided to specifically say

EAC Technical Guidelines Development Committee Conference Call Meeting on December 18, 2019

TGDC Meeting – December 18, 2019

- https://www.eac.gov/videos/eac-tgdc-conference-call-meeting-december-18-2019
- Network connections discussion 16:00 – 01:54:00
- Specific to wireless requirements: 51:00 – 57:00
- Wireless posted in March for public comment, approved by the TGDC



14.2-D – Wireless Communication Restrictions

Voting systems must not be capable of establishing wireless connections.

Discussion

Wireless connections can expand the attack surface of the voting system by opening it up to over-

254

Requirements for VVSG 2.0

February 29, 2020

the-air attacks. Over-the-air access can allow for adversaries to attack remotely without physical access to the voting system. By disallowing wireless capabilities in the voting system, this limits the attack surface and restricts any network connections to be hardwired.

This requirement does not impact or restrict the use of assistive technology (AT) within the polling place. Voters with wireless AT may have to use an adapter that leverages the 3.5 mm headphone jack.

Related requirements:	15.4-C – Documentation for disabled wireless 8.1-E – Standard audio connectors
Applies to:	Voting System

14.2-E – Wireless network status indicator

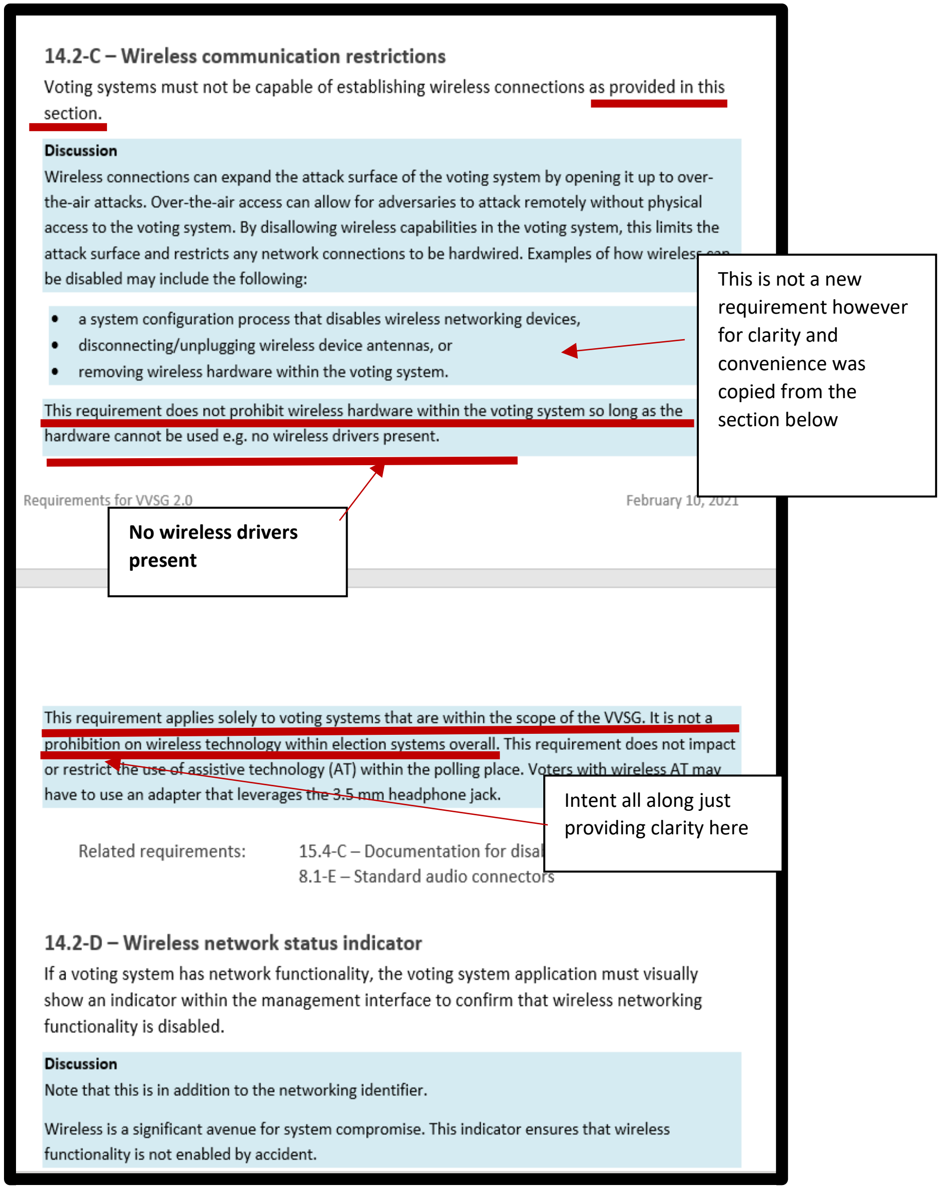
If a voting system has network functionality, the voting system application must visually show an indicator within the management interface when wireless networking functionality is enabled and disabled.

Discussion

Note that this is in addition to the networking identifier.

Wireless is a significant avenue for system compromise. This indicator ensures that wireless functionality is not enabled by accident.

Wireless Section- posted March 2020



14.2-C – Wireless communication restrictions

Voting systems must not be capable of establishing wireless connections as provided in this section.

Discussion

Wireless connections can expand the attack surface of the voting system by opening it up to over-the-air attacks. Over-the-air access can allow for adversaries to attack remotely without physical access to the voting system. By disallowing wireless capabilities in the voting system, this limits the attack surface and restricts any network connections to be hardwired. Examples of how wireless can be disabled may include the following:

- a system configuration process that disables wireless networking devices,
- disconnecting/unplugging wireless device antennas, or
- removing wireless hardware within the voting system.

This requirement does not prohibit wireless hardware within the voting system so long as the hardware cannot be used e.g. no wireless drivers present.

This is not a new requirement however for clarity and convenience was copied from the section below

Requirements for VVSG 2.0

February 10, 2021

No wireless drivers present

This requirement applies solely to voting systems that are within the scope of the VVSG. It is not a prohibition on wireless technology within election systems overall. This requirement does not impact or restrict the use of assistive technology (AT) within the polling place. Voters with wireless AT may have to use an adapter that leverages the 3.5 mm headphone jack.

Intent all along just providing clarity here

Related requirements:	15.4-C – Documentation for disal 8.1-E – Standard audio connectors

14.2-D – Wireless network status indicator

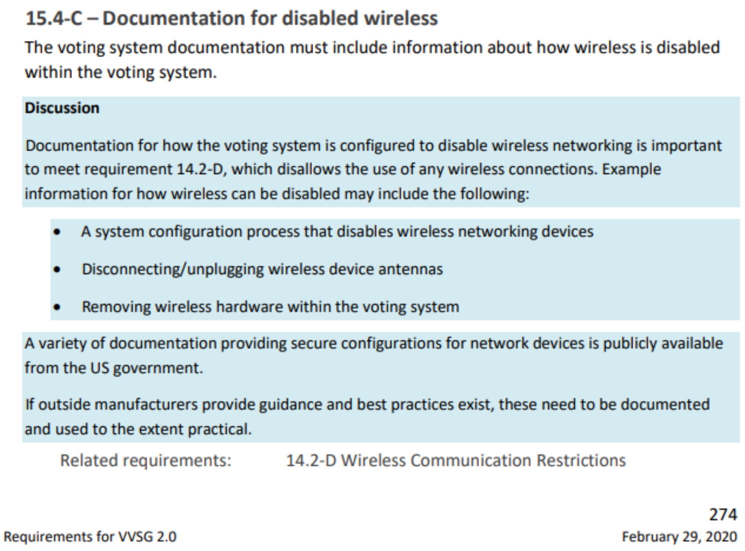
If a voting system has network functionality, the voting system application must visually show an indicator within the management interface to confirm that wireless networking functionality is disabled.

Discussion

Note that this is in addition to the networking identifier.

Wireless is a significant avenue for system compromise. This indicator ensures that wireless functionality is not enabled by accident.

Wireless Section Jan 2021



15.4-C – Documentation for disabled wireless

The voting system documentation must include information about how wireless is disabled within the voting system.

Discussion

Documentation for how the voting system is configured to disable wireless networking is important to meet requirement 14.2-D, which disallows the use of any wireless connections. Example information for how wireless can be disabled may include the following:

- A system configuration process that disables wireless networking devices
- Disconnecting/unplugging wireless device antennas
- Removing wireless hardware within the voting system

A variety of documentation providing secure configurations for network devices is publicly available from the US government.

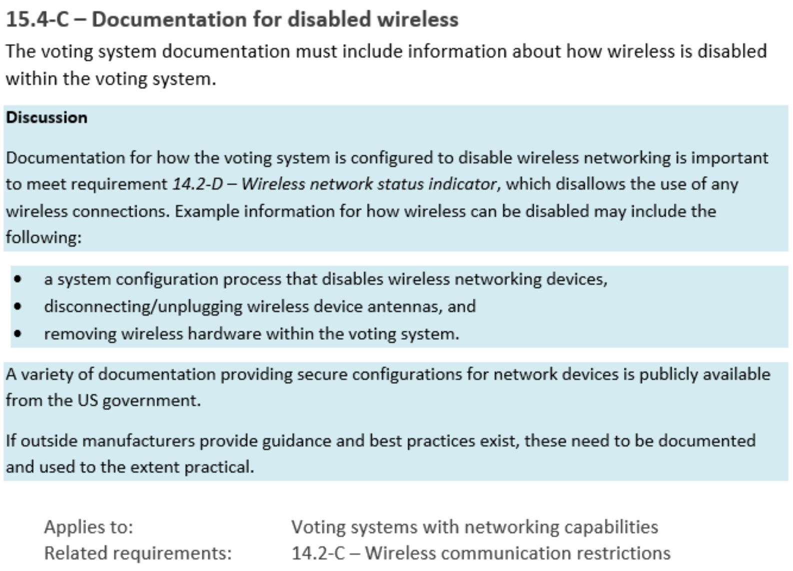
If outside manufacturers provide guidance and best practices exist, these need to be documented and used to the extent practical.

Related requirements:	14.2-D Wireless Communication Restrictions

274

Requirements for VVSG 2.0 February 29, 2020

15.,4-C Posted in March 2020



15.4-C – Documentation for disabled wireless

The voting system documentation must include information about how wireless is disabled within the voting system.

Discussion

Documentation for how the voting system is configured to disable wireless networking is important to meet requirement *14.2-D – Wireless network status indicator*, which disallows the use of any wireless connections. Example information for how wireless can be disabled may include the following:

- a system configuration process that disables wireless networking devices,
- disconnecting/unplugging wireless device antennas, and
- removing wireless hardware within the voting system.

A variety of documentation providing secure configurations for network devices is publicly available from the US government.

If outside manufacturers provide guidance and best practices exist, these need to be documented and used to the extent practical.

Applies to:	Voting systems with networking capabilities
Related requirements:	14.2-C – Wireless communication restrictions

15.,4-C Posted in January 2021