CENTER FOR DEMOCRACY & TECHNOLOGY

Testimony of

Joseph Lorenzo Hall, PhD
Chief Technologist
The Center for Democracy & Technology[1]

Hearing on "Voluntary Voting System Guidelines 2.0"
U.S. Election Assistance Commission

May 20, 2019

Chairwoman McCormick, Commissioners:

Thank you for the opportunity to speak to you today about the Voluntary Voting System Guidelines, version 2.0 (VVSG 2.0).

My name is Joseph Lorenzo Hall,[2] I'm the Chief Technologist at the Center for Democracy & Technology (CDT). I oversee CDT's Election Security and Privacy project, which focuses on educating the elections community about cybersecurity concepts and practices through a set of online interactive courses, "Election Cybersecurity 101" field guides, and by holding regular briefings and trainings for election officials, legislative staff, and journalists.

The VVSG Has Come Far, But Must Evolve Further

During my doctoral and postdoctoral work between 2004 and 2011, on behalf of the National Science Foundation's ACCURATE center (A Center for Correct, Usable, Reliable, Accurate, and Transparent Elections), I was responsible for channeling expert input into public comments on each set of the VVSG and the Voting System Testing and Certification Program manual.[3] In the time since 2004, we have

---

[1] The Center for Democracy & Technology (CDT) is a nonpartisan nonprofit public interest advocacy organization that works to advance human rights online, and is committed to finding forward-looking and technically sound solutions to the most pressing challenges facing users of electronic communication technologies. With expertise in law, technology, and policy, CDT promotes policies that protect and respect users' fundamental rights to privacy and freedom of expression, and enhance their ability to use communications technologies in empowering ways. CDT has testified in front of Congress numerous times in its over 25-year history and is a highly trusted voice in technology policy. Please direct additional inquiries to me via email (joe@cdt.org) or phone (+1-202-407-8825).

[2] My curriculum vitae is here: https://josephhall.org/HallJosephResume.pdf.

[3] Deirdre K. Mulligan and Joseph Lorenzo Hall, *Preliminary Analysis Of E-Voting Problems Highlights Need For Heightened Standards And Testing*, National Research Council's Committee on Electronic Voting (2004), available at: https://josephhall.org/papers/NRC-CSTB_mulligan-hall_200412.pdf; Erica Brand, Cecilia Walsh, Joseph Lorenzo Hall and Deirdre K. Mulligan, *Public Comment on the 2005 Voluntary Voting System Guidelines*, submitted to the U.S. Election Assistance Commission on behalf of ACCURATE and listed affiliates by the Samuelson Law, Technology and Public Policy Clinic (2005), available at: https://josephhall.org/papers/2005_vvsg_comment.pdf; Aaron Burstein, Joseph Lorenzo Hall,

seen the EAC, the VVSG, and the voting system testing and certification program change immensely for the better. Where it was originally a closely-guarded and highly-opaque system, it is now well-documented, much more effective, and it much better suits the needs of election officials, voting system manufacturers and the public, each of whom use information about voting system certification and their performance testing against common technical standards.

Adoption of the VVSG 2.0 guidelines and principles is an important opportunity to ensure that the voting system testing and certification program remains flexible and can continue to evolve with technical requirements adapting to meet the principles identified in the VVSG 2.0.

Important Considerations for VVSG 2.0

As the EAC moves to adopting and implement the VVSG 2.0 principles and guidelines, here are a number of important considerations from CDT's perspective:

1. **Principles vs. requirements:** The elections community is heartened to see the EAC with a full slate of commissioners and, crucially, a quorum with which to conduct regular business. The most critical aspect of developing and adopting the VVSG 2.0 is the need to design it to be flexible and agile, even when a quorum doesn't exist. The currently proposed "two-level" structure specifies principles and guidelines at a high level separately from requirements, at a much lower level. In this model, the principles would be somewhat like a constitutional document of the voting system testing and certification program, outlining high-level ideas that should be relatively stable over time as new voting technologies come and go. Requirements would instead specify at a much lower-level the necessary elements of a testing and certification program. If past voting system standards are any indication, the number of requirements will be large; voting systems are complex systems. Any flexibility and adaptability of this new system would be lost if EAC commissioners had to vote on more than a handful of requirements.

   We suggest that the EAC defines a separate process that outlines ongoing and regular public

---

Deirdre Mulligan, *Public Comment on the Manual for Voting System Testing & Certification Program*, submitted to the U.S. Election Assistance Commission on behalf of ACCURATE and listed affiliates by the Samuelson Law, Technology and Public Policy Clinic (2006), available at: https://josephhall.org/papers/ACCURATE_VSTCP_comment.pdf; Aaron Burstein and Joseph Lorenzo Hall, *Public Comment on the Voluntary Voting System Guidelines, Version II (First Round)*, submitted to the U.S. Election Assistance Commission on behalf of ACCURATE by the Samuelson Law, Technology and Public Policy Clinic (2008), available at: https://josephhall.org/papers/accurate_vvsg2_comment_final.pdf (ACCURATE VVSG II comment); Aaron Burstein and Joseph Lorenzo Hall, *Public Comment on the Voluntary Voting System Guidelines, Version 1.1*, submitted to the U.S. Election Assistance Commission on behalf of ACCURATE (2009), available at: https://josephhall.org/papers/accurate_vvsgv11_comment.pdf (ACCURATE VVSG 1.1 comment); Joseph Lorenzo Hall, *Public Comment on the Voting System Testing and Certification Program Manual, v2.0*, submitted to the U.S. Election Assistance Commission on behalf of ACCURATE (2011), available at: https://josephhall.org/papers/accurate-vstcp2-comment.pdf.

comment for VVSG requirements and a mechanism for members of the TGDC and EAC staff to flag requirements that might require Commission deliberation, discussion, or vote.

2. **Transitioning from one VVSG testing regime to another:** A voting system testing standard does not provide much assurance if systems can be certified against vastly outdated standards developed many years ago. The new two-level VVSG structure will allow requirements to evolve in time, but in order for the underlying systems to also evolve, the testing and certification program must set hard boundaries past which any new voting system submissions must be certified against newer requirements.

   Because voting systems are now tested as wholistic *systems* and not as individual *components*, and because they are certified against large monolithic standard specifications (e.g., the VVSG 1.1) instead of a frozen subset of continually evolving requirements, some current systems are performing wildly outside the expectations of election officials and users, for example display lag times associated with computers of twenty years ago.[4] Instead, manufacturers should be required to commit to a dated "snapshot" (a subset) of VVSG requirements – for example, "all approved requirements for precinct-based optical scanning systems dated January 1, 2020" – and be allowed to be tested against those requirements (or any newer snapshot) for a period of 5 years. This would allow manufacturers to target a certain stable subset of requirements necessary to field a whole election system, but would require and encourage them to move to a more recent snapshot within 5 years. (This is just one candidate proposal and we encourage the EAC to solicit more ideas here, potentially in the form of a joint workshop with NIST on designing evolving voting system standards.)

3. **Adversarial testing and vulnerability handling:** Two critical properties of well-engineered modern information systems are 1) their ability to withstand scrutiny by trained security experts and 2) having an effective process in place for fixing vulnerabilities when they are inevitably found. Security is a systems property that is notoriously difficult to test, often requiring specific kinds of expertise to identify and fix serious flaws.

   Voting systems should be tested by dedicated computer and network security experts using adversarial testing methods – "penetration testing" – where a operational version of the system is attacked by an expert team trying to find bugs, flaws, and vulnerabilities.[5] These kinds of penetration testing efforts will inevitably find issues and each voting system manufacturer must have an effective vulnerability handling process and standard vulnerability reporting mechanism in place (see the ISO standards for vulnerability handling and reporting: ISO 29147/30111[6]). The testing and certification process should confirm that each manufacturer

---

[4] Adi Robertson, "Texas voting machines are switching votes — but it's bad design, not hacking", *The Verge* (October 30, 2018), available at: https://www.theverge.com/2018/10/30/18037872/texas-voting-machine-hart-eslate-voting-ballot-switch-problems.

[5] This activity is similar to a process under consideration in previous iterations of the VVSG – "open-ended vulnerability testing" (OEVT); *see* ACCURATE VVSG II comment, ACCURATE VVSG 1.1 comment, *id.*, fn. 3.

[6] ISO, ISO/IEC Standard 29147:2014, "Information technology – Security techniques – Vulnerability disclosure," (2014), https://www.iso.org/standard/45170.html; ISO, ISO/IEC Standard 30111:2013, "Information technology – Security techniques – Vulnerability handling processes," (2013), https://www.iso.org/standard/53231.html.

has an effective vulnerability handling and reporting program by tracking the reporting, handling, and resolution of bugs found in VSTL penetration testing. In addition, the EAC should hire a security testing program evaluator that could assess the quality of security testing at current Voting System Testing Laboratories (VSTLs) and potentially require them to hire outside penetration testing firms to fulfil this aspect of testing.

4. **Common Data Format:** Work on various elements of a common data format that can be shared across election systems has been going on for years.[7] Wider use of standardized common data formats could help promote a number of desirable aspects in a voting system, from *composability* – where pieces of one system can be more easily used with pieces of a second system – to *transparency* – for example, allowing election campaigns, journalists, auditors, and the public a common source of standardized election information.

   In particular, the event logging specification developed by NIST and collaborators[8] provides a starting point that, if promoted as a recommended or required element of voting system testing submissions could result in specific gains with respect to cybersecurity. Common event logs across the many systems involved in running an elections system could allow election officials and cybersecurity defenders to better understand when suspicious events may require further investigation, rather than having to make sense across wildly different, potentially proprietary log formats.

5. **Critical areas outside the scope of the VVSG:** Recent years have seen a proliferation of components of voting systems – for example, electronic pollbooks – and methods of voting – for example, voting over the internet, by email, or by fax – that are currently out of scope of the VVSG and and have few associated standards. Each of these areas could use some attention from the standards process.

   The EAC should explore extending its authority to encompass subsystems that may be commonly used with a certified voting system, even if that subsystem may not be strictly within the definition of a voting system. Unfortunately, if something is classified as an accessory to a certified voting system but that accessory can cause the voting system to fail, the accessory should be properly defined as part of the larger voting system. For example, electronic pollbooks are becoming a standard feature of modern polling places to improve the voter check-in flow and experience. However, they can have complex interactions with network resources; for example, when used in vote center deployments, they need to communicate with a central database to be able to prevent voters from being able to vote twice in different vote centers. When parts of the electronic pollbooks fail, there must be some process to ensure that voters can continue to cast votes; without that system-level protection, serious issues can happen, similar to what happened in Johnson County, IN in November 2018 where voters could not vote for four hours due to a communication problem between the electronic pollbooks and

[7] John P. Wack, Kim Brace, Samuel Dana, Herb Deutsch, John Dziurlaj, Ian Piper, Don Rehill, Richard M. Rivello, Sarah Whitt, NIST Special Publication (NIST SP) - 1500-100, *Election Results Common Data Format Specification*, (2016), available at: https://www.nist.gov/publications/election-results-common-data-format-specification.

[8] *See:* https://github.com/usnistgov/ElectionEventLogging.

the the database.[9]

Similarly, remote paperless voting methods – internet, email, fax – continue to be used without much guidance as to best practices for using these systems. While experts have substantial concerns with any form of paperless remote voting,[10] if these methods are going to be used, guidance should exist to promote technically safe use of these systems, stressing they should only be used when no other voting method is possible. As just one example, it has been best practice for years now to ensure that web-based systems use secure forms of communication, notably, the HTTPS standard.[11] If forms of internet voting exist that allow insecure communication (e.g., HTTP), this can often be easily fixed; organizations like CDT help businesses, government agencies, and NGOs move to more secure forms of communication that can reduce the ability for attackers to insert, drop, or modify data in transit.

6. **Beyond testing, standardizing practices:** Unfortunately, the testing and certification program can only do so much; procedures or ingrained practices can override important security and usability considerations to the detriment of voters. The EAC is in a good position to define a baseline set of best practices and procedures for election administration, including cybersecurity, that can begin to standardize the procedural aspects of modern voting technologies, complementing the technical voting system standards and certification process. Ideally, in addition to a certified voting system that has met some level of testing against a considered technical standard, election officials could also be given a set of comprehensive reference materials that instruct and assist them in how to configure and deploy their voting system according to best practice.

Conclusion

Once again, thank you Chairwoman McCormick and to the Commission for the opportunity to speak today, and please feel free to contact me with any additional questions.

Thank you.

---

[9] Voting System Technical Oversight Program, "A Preliminary Investigation of ES&S Electronic Poll Book Issues in Johnson County, Indiana for the 2018 General Election," *Indiana Secretary of State* (Dec. 31, 2018), https://www.in.gov/sos/elections/files/Report%20-%20Johnson%20County%20ePB%20Investigation%20Dec%2031%202018.pdf.

[10] National Academies of Sciences, Engineering, and Medicine. 2018. *Securing the Vote: Protecting American Democracy*. Washington, DC: The National Academies Press. https://doi.org/10.17226/25120.

[11] White House Office of Management and Budget memorandum M-15-13, "A Policy to Require Secure Connections across Federal Websites and Web Services," (June 8, 2015), available at: https://https.cio.gov/.